MILITARY ACADEMY

DEPARTMENT OF POSTGRADUATE STUDIES

INTEGRATION OF INTELLIGENCE TECHNIQUES ON THE EXECUTION OF PENETRATION TESTS (iPENTEST)

Fábia Filipa Aires Berbigão

Master's Thesis to obtain the degree of

Master in Information Warfare and Competitive Intelligence

Lisbon

2018

MILITARY ACADEMY

DEPARTMENT OF POSTGRADUATE STUDIES

INTEGRATION OF INTELLIGENCE TECHNIQUES ON THE EXECUTION OF PENETRATION TESTS (iPENTEST)

Fábia Filipa Aires Berbigão

Master's Thesis in Information Warfare and Competitive Intelligence

Work carried out under supervision:

Supervisor: Professor Rui Miguel Silva from Lab UbiNET of the Polytechnic Institute of Beja

Co-Supervisor: Professor Luís Alexandre Madureira, professor at the Military Academy

Lisbon

2018

ACKNOWLEDGEMENTS

À semelhança da teoria de Lacord, quaisquer que sejam as pessoas que se cruzem na nossa vida, mesmo que inconscientemente, deixam um pouco de si e levam um pouco de nós. Sendo esta a prova de que cada pessoa é insubstituível e incomparável.

A mais subtil Responsabilidade da vida é a de estruturar condições para os encontros não aleatórios entre almas destinadas a compartilhar experiências de vida.

Deixo expressos os meus sinceros agradecimentos ao meu orientador, professor Rui Miguel Silva, cujos ensinamentos e reflexões transmitidas foram imprescindíveis para a realização desta dissertação de mestrado, e também para a minha expansão intelectual.

É uma honra ter vivido intensivamente esta experiência consigo!

Ao professor Luis Madureira, cujo seu conhecimento e dinâmica em sala de aula são referências de excelência para todos aqueles que desejem aprimorar os seus conhecimentos em Competitive Intelligence.

Não conseguirei encontrar forma de expressar o sentimento de gratidão a todos aqueles que, de uma forma ou de outra, foram uma presença constante nesta etapa da minha vida e cujo apoio foi o motor e a motivação necessária para tornar possível a concretização deste meu objectivo.

À Inês, cuja coragem e força de espírito inigualável é uma fonte de inspiração incalculável para seguir sempre a voz da minha essência. Agradeço o teu apoio nas diversas dimensões da minha vida e em especial pela tua inestimável contribuição para esta dissertação. Estou profundamente grata ao Universo pela tua presença na minha vida.

Em especial aos meus pais, a quem serei eternamente grata por todos os valores transmitidos, pela incansável dedicação e presença incondicional em todos os momentos da minha existência.

Vocês preenchem a minha vida e o meu coração com amor e significado!

fábiz filipa Berbigão

18/11/18

*"**Imagination is** more **important** than knowledge.*

For while knowledge defines all we currently know and understand,

*imagination **points to all we might yet discover and create**"*

Albert Einstein (1929)

INDEX

INDEX OF FIGURES

INDEX OF TABLES

ABSTRACT

Penetration Tests (*Pentests*) identify potential vulnerabilities in the security of computer systems via security assessment. However, it should also benefit from widely recognized methodologies and recommendations within this field, as the *Penetration Testing Execution Standard* (PTES). The objective of this research is to explore PTES, particularly the three initial phases: 1. *Pre-Engagement Interactions; 2. Intelligence Gathering; 3. Threat Modeling;* and ultimately to apply Intelligence techniques to the Threat Modeling phase. To achieve this, we will use open-source and/or commercial tools to structure a process to clarify how the results were reached using the research inductive methodology. The following steps were implemented: i) critical review of the "Penetration Testing Execution Standard (PTES)"; ii) critical review of Intelligence Production Process; iii) specification and classification of contexts in which Intelligence could be applied; iv) definition of a methodology to apply Intelligence Techniques to the specified contexts; v) application and evaluation of the proposed methodology to real case study as proof of concept. This research has the ambition to develop a model grounded on Intelligence techniques to be applied on PTES Threat Modeling phase.

Keywords: *Intelligence; Pentesting; PTES; Structured Analytic Techniques; Threat Modeling.*

GLOSSARY

Part I – List of Abbreviations and Acronyms

BEI – *Biometrics-enabled Intelligence*

CCA – *Cross-Consistency Assessment*

CCM – *Cross-Consistency Matrix*

CI – *Counterintelligence*

CIA – *Central Intelligence Agency*

DOMEX – *Document and Media Exploitation*

FEI – *Forensics-enabled Intelligence*

GMA – *General Morphological Analysis*

GMI – *General Military Intelligence*

HUMINT – *Human Intelligence*

HVAC – *Heating, ventilation, and air conditioning*

I2 – *Identity Intelligence*

IMINT – *Imagery Intelligence*

ISHD – *Islamic State Hacking Division*

ISSAF – *Information Systems Security Assessment Framework*

MASINT – *Measurements and Signatures Intelligence*

NIST – *National Institute of Standards and Technology*

OIR – *Other Information Requirements*

OSINT – *Open Source Intelligence*

OWASP – *Open Web Application Security Project*

PeI – *Pre-engagement Interactions*

PENTEST – *Penetration Test*

PENTESTER– *Penetration Tester*

PIR – *Priority Intelligence Requirement*

PTES – Penetration *Testing Execution Standard*

S&TI – *Scientific and Technical Intelligence*

SAT – *Structured Analytical Techniques*

SE – *Social Engineering*

SIGINT – *Signals Intelligence*

SIRP – *Information Services of Portuguese Republic*

SMB – *Small and Medium-sized Businesses*

SOCMINT – *Social Media Intelligence*

TECNHOINT – *Technological Collection*

Part II – Terms and Definitions

Active Intelligence Gathering – This type of intelligence gathering should be detected by the target and identified as suspicious or malicious behaviors. Information about network infrastructure, open ports other vulnerabilities should be identified.

Blind test – On this type of security testing the Pentester has no prior knowledge of the testing subject. However, the target is prepared for Pentesting, knowing in advance all its details. This scenario measures the performance and skills of the Pentester. Also known as **War Gaming** or **Role Playing**.

Collection Plan – Systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements.

Cross Consistency Assessment – Process by which the attributes values in the morphological field are compared with one another, pair-wise, into a cross-impact matrix (CCM). As each pair of values is examined, a judgement is made to understand if the pair can coexist, representing a consistent relationship.

Cyber knowledge – The proficiency related to computers, information networks, or automated systems.

Double Blind test – On this type of security testing the Pentester has no prior knowledge of the testing subject. Also, the target is not notified in advance about the scope, channels and vectors to be tested. This scenario tests both teams' skills and preparedness to unknown variables. Also known as **Black-box test** or **Penetration test**.

Double Gray Box test – On this type of security testing the Pentester has limited knowledge about its defenses and assets and full knowledge about channels. The target is notified in advance about the scope and audit time frame. However, the channels that will be tested or the test vectors are not given to the target. This scenario tests both skills and preparedness of the Pentester and the target. Also known as **White Box Test**.

Gray Box test – On this type of security testing the Pentester has limited knowledge of its defenses and assets and full knowledge of channels. This test is often performed by the target itself to get a self-assessment of the internal system. The target is prepared for Pentesting, knowing in advance all its details. This scenario measures the skills and knowledge of the Pentester to unknown variables. Also known as **Vulnerability Test**.

Human Intelligence – A category of Intelligence derived from information collected and provided by human sources. Also known as **HUMINT.**

Imagery Intelligence – A category of Intelligence derived from the collection of images from a variety of platforms. Also called **IMINT**. Comprising either individually or in combination the Photo Intelligence (PHOTINT) and Geospatial Intelligence (GEOINT).

Kinetic knowledge – The proficiency related to physical systems, motion of bodies, and forces associated with that movement.

Measurement and Signature Intelligence – A category of Intelligence derived from analysis and treatment of data and information (quantitative and qualitative) obtained through sensors. Associated to the transmitters or receivers through the measurement of specific parameters. Also known as **MASINT**. Comprising either individually or in combination frequency sensors of the electromagnetic spectrum, such as radio, nuclear, acoustic, seismic and optical frequencies.

Morphological Field – The field of constructed dimensions or attributes which is the basis for a morphological model.

Morphological Model – A morphological field with its attributes assessed and linked through a Cross-Consistency Assessment (CCA).

Open Source Intelligence – A category of Intelligence which involves gathering and acquiring information from open sources and then using it to reform legal intelligence. Also Called **OSINT**.

Passive Intelligence Gathering – It is used when the target is required not to detect the information gathering. In this situation, one should not interact with the target. Therefore, the information gathering should concentrate on archived or stored information. However, non-updated information represents a limitation.

Reversal test – On this type of security testing the target has full knowledge of its processes and operational security, but has no information about what, how, or when the Pentester will be testing. This scenario tests the preparedness of the target to unknown variables and vectors of agitation. Also known as **Red Team exercise.**

Semi-Passive Intelligence Gathering – The interaction with the target must avoid detection in the alarm sensors. It should not appear as unusual Internet traffic and behavior. Depth reverse

lookups or brute force attacks should not be performed. The aim is to look for document metadata or published files, without drawing attention to the performed activities.

Signals Intelligence – A category of Intelligence derived from communications, electronic, and foreign instrumentation signals. Also known as **SIGINT.** Comprising either individually or in combination all the Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

Social Media Intelligence – A category of Intelligence built upon tools and solutions for social media monitoring. Also known as **SOCMINT**. Signal and Data inputs in social networks are processed into meaningful actionable intelligence.

Tandem test – On this type of security testing both Pentester and target are prepared and know in advance all Pentesting details. This test aims to assess how strong are the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables. This is also known as **Crystal Box Test**.

1. INTRODUCTION

Over the last decades great technological advances have changed societies. Almost every person adopted these technologies, leading to undergoing structural changes. The development of Internet and technology in a comprehensive way, brought great opportunities. For instance, brought the possibility to have all kind of information at a click of distance and to connect people from another side of the globe, crossing over all existing geographical and temporal limitations. Yet, it also brought new challenges, leading organizations to re-evaluate their structure, processes and their own internal culture. The pace of technological advancement is growing fast, and consequently the volume and velocity of data is growing exponentially, leading to a society with a permanent need of information (**Braga, 2000**).

Across the business sector, an understanding about how to get the most value from data is being asked. Data and information can be used to obtain actionable customer perceptions that helps drive new incomes and most important to strengthen the cybersecurity of its systems. Data and Information are a vital resource and an influence to reach superiority in every context. Acquire quality, reliable, timely and actionable information (information that adds value) makes possible to challenge preconceive limits. And it also makes possible for businesses, to develop a greater robustness to critical decision-making, such as decisions over its security, and potential existing risks to its assets (**Goldman, 2006**).

Yet, the majority of businesses are not prepared to use the available data and information to protect them against cyber threats. Data is the new oil, information is the new gold and Cybercriminals will seek for it. It has become easier to be behind a computer with the amount of available options to become anonymous in the cyberspace. Also, the accessibility to cyber weapons, that makes possible for a single person to attack any business from another side of the globe, led criminals to invest improving of their cybernetic skills.

The biggest concern of this research is to find ways to contribute to prevent Internal and External threats to access business systems. Threats are becoming more sophisticated and frequent. Therefore, it would be important for organizations to have mechanisms protecting them from threats.

There is a lot of security information being gathered and disseminated about security events, and also about computer and network systems characteristics. This information should be used to assess the security maturity level and to implement the right mechanisms to protect organization's critical assets.

The great yearning of getting new trends, such as trendy software's that generate financial profits, leads CEO's to view the security issues as a secondary concern. Every existing gap in security may be exploited by cybercriminals. Therefore, security should be the first concern in every business and organizations. So, we should shift perspective and start now being concerned about the security.

Soon, business environment will be almost unrecognizable. Everything that can be connected will be in short-time, which will bring great efficiency to business processes. If we add artificial intelligence (AI) based in software and services, then business efficiency will be enormous. But without a strong security maturity level, businesses may suffer chaotic damages, and our biggest concern is to understand what can be done to protect businesses from external threats and internal threats.

Because Portuguese business community consist in small and medium-sized (SMB), companies will not be able to invest in high-technology to protect their critical assets. However, these assets are critical for any business sustainability and for this reason this research concern was to find an approach to modeling cybernetic and non-cybernetic threats.

One approach SMB should take to protect their assets and assess its security maturity level is to use recognized Pentesting recommendations such as PTES. To clarify about business's risk propensity and enabling the Pentester to closely emulate security incidents, PTES recommends the construction of a threat modeling model using the existing internal and external data and information (**Nickerson et al., n.d.).**

From the exposed reality, we suggest to carry out this research, focusing on mechanisms to create a Threat Profiling and project potential Threat Scenarios using the existing Data and Information. The result of this research, iModeling, is a threat modeling model, with the three following functions: (1) Scenario-based Forecasting; (2) Business risk Assessment; and (3) Offensive Scenario-based approach; which will be explained in detail further in this research.

1.1. Research Methodology

Based on the "fundamental principles of the scientific process" (**Quivy & Campenhoudt, 2005**), in the development of this project development of this project and to investigate its problematic question, we adopted the inductive approach, also known as inductive reasoning. It can be understood as a mental process, based on particular and verified data, where a general or universal truth is deduced. Therefore, the purpose of inductive arguments is to lead to conclusions which content is much wider than the premises on which they were founded (**Lakatos & Marconi, 2003).**

Important to the current research, inductive approaches do not imply the formulation of theories or hypotheses on the beginning of the research and researchers are free to alter the direction of the study after the research process begins (**Saunders, et al, 2012**).

During the present research we used mixed research methods, such as documental analysis and expert interview.

1.2. Research Objectives

This research, which results in a Master's dissertation in the field of "Information Warfare and Competitive Intelligence", aims to qualitatively contribute to this field by articulating and integrating knowledge learned throughout the curricular part of the master's degree. Additionally, in order to effectively and practically apply the obtained results on the real world, this research has the quantitative objective of developing a methodology for applying in PTES threat modeling phase.

There are, however, intermediate objectives that together will enable the qualitative and quantitative objectives to be achieved: i) critical review of the "Penetration Testing Execution Standard" (PTES); ii) critical review of Intelligence Production Process; iii) specification and classification of the contexts in which Intelligence is applied; iv) definition of a methodology to apply Intelligence Techniques on the specified contexts; v) application of the proposal methodology to a real case study as proof of concept.

1.3. Research Motivations and Relevance

This research founded its motivations in our personal academic experience in Pentesting, and professional experience in Criminal Intelligence, in particularly Digital Forensic Intelligence Investigation. With the growth of cyber-attacks in the past years, it is more important than ever to undertake systematic Penetration Tests on identifying weaknesses

before attackers. Pentesting should benefit from recognized methodologies and frameworks to keep the process consistent and repeatable, such as the Penetration Testing Execution Standard (PTES). The PTES recommendation does not benefit from a specific model to execute the Threat Modeling phase, although it requires the construction of a consistent model in specific terms with the ability to be replicable on future tests (**Nickerson et al., n.d.**). Pointing this as a gap on PTES literature, we considered it a pertinent topic for which we propose the development of a model, based on Intelligence techniques, to apply to the PTES Threat Modeling phase. The proposed model aims to assess potential risks and threats according to the organizations' critical assets, supporting Pentesters to discover an efficient way to attack its target.

The result of this research – a threat modeling model – could be applied by Pentesters not only in the scope of traditional computer systems, but also by Cyber Intelligence Investigators and professionals of other fields of application related to security and disaster recovery from several branches of the business sector.

1.4. Statement of the Problem

The main question (CQ) we pretend to explore is the following: **Could the Intelligence process be systematized, identifying methodologies, techniques, and tools to build a model for the PTES recommendation Threat's Modeling phase?**

To divide the central question into specific questions, we propose the following three research sub questions (SQ):

- SQ1 – **Could it be possible to identify common features of application between Intelligence process and other domains?**
- SQ2 – **Could it be possible to identify methodologies, techniques, and tools that better adapt to specific Intelligence needs?**
- SQ3 – **Could it be possible to apply Intelligence methodologies and techniques to build a Threat Modeling model?**

1.5. Research Limitations and Difficulties

During this research, some limitations were found, mainly regarding the scarce of scientific approaches about Intelligence. The lack of available data led to significant obstacles on finding recent academic publications. This occurs because Intelligence is closely related to undercover activities, and mostly spoken by people related to secret agencies. Only after the

failure of September 11 Intelligence started to arise online. Also, it was by that time that official military documents started to be released, becoming available to public in general, and thus contributing to the academic field. For these reasons, it was difficult to find recent academic publications relating Intelligence to other fields of application, such as computer security. On the contrary, it was possible to find several theoretical and technical references in the scientific field of Penetration tests. However, academic references, particularly concerning PETS recommendation, revealed to be a tough task to accomplish. Most of the references about PTES directs to PTES official website, a "Wiki" designed by a group of information security practitioners and experts from all areas of the industry around the globe. Taken together, the lack of academic publications, and even the variety of sources of information for both concepts characterize this research as having lack of prior research studies correlating Intelligence and Pentesting. For this reason, it was challenging to find a logical and coherent way to merge harmoniously Intelligence techniques with PTES recommendation while having reliable scientific references supporting.

1.6. Structure and Synthesis of Chapters

This research is divided into five parts described as follows:

- Chapter 1 covers the introduction, research relevance and delimitations, problematic question, objectives and research methodology approach.
- Chapter 2 covers the state of art that has two vital branches. The first consists in a critical review of Pentesting with focus on the three initial phases of PTES recommendation. The second consists in the critical review of Intelligence, its cycle and structured analytic techniques, on which we based to create the iPentest model.
- Chapter 3 covers the result of the research – the iPentest model. On this chapter, we offer a detailed explanation of iPentest methodology for iPlanning and iModeling phases. Particularly, in the iModeling phase we present an Incident Profiling framework and its operationalization based on Intelligence techniques, resulting in the iModeling model – an Incident Profiling model.
- Chapter 4 covers the evaluation of iModeling using real case studies as proof of concept.
- Chapter 5 covers the conclusions, relevant considerations about the research, its limitations, an evaluation of the initial questions, and an appreciation for future investigations on the development of iModeling.

2. RELATED WORK

This chapter is divided into two parts: the first is dedicated to the analyzes of the penetration tests contributions, contexts and its methods of execution. We will detailly explore the PTES recommendations focusing on the three initial phases (*1. Pre-engagement Interactions; 2. Intelligence Gathering; 3. Threat Modeling)*. This will be the foundation to develop our research. The second part is dedicated to characteristics and considerations of Intelligence, in order to look for a new approach on understanding this concept. Additionally, we will undertake a critical analysis of the traditional cycle of Intelligence by thoroughly exploring its phases.

2.1. Penetration Tests

Pentesting consists in conducting security assessments on which an auditor (Pentester) employs the same techniques of a real attacker (hacker). The goal is to identify potential vulnerabilities or configuration failures that could lead to a breach on the security measures of computer science systems', such as network infrastructures, wireless segments, websites, web and mobile app, and human or physical components (**Dinis, 2013**).

However, there are other Pentest's specific domains, such as critical infrastructures, that in many cases use owner communication protocols – which are known as protocols that are mainly designed and implemented by the manufacturer – therefore, they are not publicly available. Another growing concern, or even potential target, is the Internet of Things (IoT) security. Few years ago, if we would say that a phone could be used to copy a fingerprint none would believe it. Nonetheless, today it is possible to say that, for instance, hackers with a malicious intention can use a fridge to break into bank accounts. This is known as Era of The Internet of Things and it is growing at a dangerously fast speed. For instance, on 17th July 2017, the FBI reported a case about Smart Toys (**FBI, 2017**), made to entertain children. It contains sensors, microphones, cameras, data storage and other multimedia capabilities, including voice recognition, GPS locations and Internet connection (via Wi-Fi or Bluetooth) capable of being controlled by an Android or IOS mobile device. The lack of security measures, such as performing periodic Pentests, put in risk children's privacy and safety due to the amount of personal information that is involuntarily revealed.

Pentesting is part of a preventative approach that ensure that vulnerabilities are not exploited. It assesses the reaction capability of any information technology (IT) system identifying the

technological capabilities that hackers need to successfully compromise that system. In this sense, Pentesting allows to identify system's vulnerabilities, making it possible to implement suitable security measures to detect, prevent and mitigate potential threats (**NIST SP 800-115**).

It is a good practice to keep the Pentesting process consistent and auditable through recognized methods and recommendations, developed by experts in this field. The following recommendations are historically the most well-known:

- **OSSTMM** – Open Source Security Testing Methodology Manual (**2000**)
  - [Institute of Security and Open Methodologies]
- **OWASP ASVS** – OWASP Application Security Verification Standard Project (**2001**)
  - [OWASP Foundation]
- **NIST SP 800-115** – Technical Guide to Information Security Testing and Assessment (**2008**)
  - [National Institute of Standards and Technology]
- **ISSAF** – Information Systems Security Assessment Framework **(2006)**
  - [Open Information Systems Security Group]
- **PTES** – Penetration Testing Executing Standard (**2009)**
  - [Group of Information Security Practitioners]

The table below summarizes the main contributions related to recommendations in Pentest's domain, already mentioned above.

RECOMENDATION	HISTORIC	MAIN CONTRIBUTIONS
OSSTMM	✓ v.1 (**2000**) ✓ v.2.1 (**2003**) ✓ v.2.2 (**2006**) ✓ v.3.0 (**2010**)	✓ **Characterizes SegOp** through an **analysis** and **correlation** of the results. ✓ The methodology benefits 6 types of tests: *1. Double Blind; 2. Tandem; 3. Reversal; 4. Blind; 5. Gray Box; 6. Double Gray Box;* ✓ Assess the safety of the following modules: information; processes; Internet technologies; communication; wireless; physique.
OWASP ASVS Project	✓ V1.0 (**2009**) ✓ v2.0 (**2014**)	✓ The standard provides a basis for testing application technical security controls and technical security

	✓ v3.0 (**2015**) ✓ v3.0.1 (**2016**) ✓ v.3.1 (**2018**) (spreadsheet only)	controls in the environment, which can be used as a metric and guidance, and during a procurement. ✓ It has three application security verification levels: Level 1 meant for software; Level 2 for applications that contain sensitive data; Level 3 for critical applications that perform high value transactions and sensitive data, such as medical data.
ISSAF	✓ v.0.1.5 (**2005**) ✓ v.0.2.1. (**2006**)	✓ A methodology of safety assessment, formed by two documents: one that focus on the aspects of business security and the other on penetration tests with a framework centralized on the tools. ✓ Consists in **three sections**: 1. *Planning & Preparation; 2. Assessment (9 steps); 3. Reporting, Clean-up & Destroy Artefacts*.
NIST SP 800-115	✓ SP 800-115 **(2008)**	✓ Recommendation with **technical aspects** to check **the SegInfo** assessment. It has models, techniques and tools that can be used to assess various types of systems and situations, and allows a cyclic process to assess security. ✓ The recommendation has a simplified methodology with **four** sections: 1. *Planning; 2. Discovery; 3. Execution; 3. Post-Execution.* ✓ **Includes guidelines** for: the security politics; the role of the administration in the security tests; the techniques of security review; the identification and systems analysis; the vulnerability assessment and analysis; vulnerability validation; Planning SegInfo tests; do security tests; post-test activities.
PTES	✓ PTES (**2009**) ✓ PTES (**2018**)	✓ This recommendation proposes of systematization of the entire Pentest process with a **sequence of procedures** and alerts for **considering a set of aspects.** ✓ The recommendation has seven stages: *1. Pre-engagement Interactions; 2. Intelligence Gathering; 3. Threat Modeling; 4. Vulnerability Analysis; 5. Exploitation; 6. Post Exploitation; 7. Reporting.* ✓ It's directed to perform Pentests on: network infrastructures; websites; web-applications.

Table 1 – Pentests Main Contributions

Despite the main contributions previously identified, these recommendations also have some limitations: some are very comprehensive or are outdated. For instance, regardless of OSSTMM evolution, it has taken a holistic approach (both for testing a GSM system and for a computer system), converting it into a wide recommendation for the object under analysis.

The main advantage is that it explains very well its scenarios (1. Double Blind; 2. Tandem; 3. Reversal; 4. Blind; 5. Gray Box; 6. Double Gray Box). However, authors have pointed as disadvantages a steep learning curve and a paid subscription to access to the latest version v4 (**Herzog, 2001**).

OWASP ASVS Project consists in a checklist – with level 1 (opportunistic), 2 (standard) and 3 (advanced) – of items that should be covered by an application security test. Each level increases the complexity and quantity of tests which can be applied to web and mobile applications. OWASP ASVS is not a methodology to execute Pentesting, it is a granular checklist containing tests that are expected to be done (**OWASP ASVS, 2016**).

ISSAF attempts to cover all possible domains of Pentesting from beginning to conclusion. It explains the distinct relationships between tasks, being focused on the tools and its tutorials. However, because there haven't been new developments since 2006, the tools are outdated (**ISSAF, 2006**).

NIST recommendation make suggestions about physical security, such as physical theft of a critical device of a company, also considering social engineering, such as impersonating an employee of a company and asking for logins systems (**NIST SP 800-115**).

Finally, the PTES recommendation is a very thorough methodology to perform Pentests, consisting in a sequence of seven detailed phases that warns about technical as well as other important aspects of a Pentest, such as scope and reporting. It has detailed instructions on how to perform the required tasks to test the security at any environment. PTES takes an advantage over other recommendations, because it is inclusive of the most commonly found technologies and also includes not so common ones. Additionally, PTES incorporates other frameworks within it, it is easy to understand, adaptable to personalized Pentesting needs and frequently updated (**Nickerson et al., n.d.**).

For these reasons this research was conducted based on the PTES recommendation.

2.1.1. Penetration Testing Execution Standard - PTES

PTES is one of the most acknowledged recommendation to execute Pentests, designed to provide both businesses and security service providers with a common language and scope for executing Pentests at any environment. PTES consists in seven phases that clarify this test efficacy, covering everything related to a Pentest. However, this section will only focus on the three first phases, in order to understand its importance while performing a Pentest.

1. **Pre-engagement Interactions:** the aim of this section is to present tools and techniques to support the initial communication with the client and the reasoning behind the Pentest;
2. **Intelligence Gathering:** the aim of this section is to perform reconnaissance against a target to gather as much information as possible. This information will be then utilized on the threat modeling phase and when penetrating the target during the vulnerability assessment and exploitation phase. It defines Intelligence Gathering activities of a Pentest to produce a strategic attack plan;
3. **Threat Modeling:** the aim of this section is to define a threat modeling approach. This approach is required for a correct execution of a Pentest. This phase is critical to evaluate the risk appetite of the organization and prioritize and secure their critical assets;
4. **Vulnerability Analysis:** the aim of this section is to identify systems' weaknesses and applications' flaws, such as host and service misconfiguration or insecure application design, which can be exploited by the attacker. Several automatized tools can be used, such as network/general vulnerability scanning;
5. **Exploitation:** the aim of this section is to establish access to a system or resource avoiding security restrictions, performed through an attack simulation. It consists on a customized application (*exploit*), according to the previous detected flaws, in order to identify the main organization entry point and its critical assets;
6. **Post Exploitation:** the aim of this section is to determine the value of the machine compromised and guarantees the control of the machine for future events;
7. **Reporting:** the aim of this section is to define base criteria for Pentest reporting. It captures the entire process of Pentesting, including information about how to fix the organization systems' vulnerabilities, discovered by Pentest, and raise awareness about information safety.

2.1.1.1. Pre-Engagement Interaction Phase

Traditionally it is known as the "Contract phase" on which the Pentester discusses the scope, terms and depth levels of Pentest execution with the client. The main goal is to define what needs to be tested, and how to test it. To do so, the Non-Disclosure Agreement (NDA), a confidential agreement about the extracted information during the Pentest, needs to be signed. Although there are several techniques, tools and information explaining how to penetrate a network infrastructure, we conclude that there is a lack of developed approaches in Pre-Engagement Interaction phase. Neglecting this initial phase can lead Pentester to a flawed, non-completed final product, and even to trespassing the thin line of legality. Therefore, it is extremely important to inform about how to perform this phase according to the following tasks (*see annex I – PTES: Pre-Engagement Interactions*):

i. Pre-engagement Interactions/Scoping

Defining scope is one of the most important components of a Pentest but it is also one of the most overlooked tasks by Pentesters. Systems and technologies that should be tested are identified and documented. Furthermore, Pentest time estimation and costs are agreed between the Pentester and the client.

ii. Pre-engagement Interactions/Goals

Also known as "Goals Specification", is in this phase that goals are stated according to the customer needs. It is also important to evaluate the organization technological infrastructure security level. For instance, if the organization has a low security level it is strongly recommended the execution of a previous vulnerability analysis, instead of a complete Pentest.

iii. Pre-engagement Interactions/Testing Terms & Definitions

The Pentester should have the ability to use an understandable language with the customer while explaining the technical terms and concepts.

iv. Pre-engagement Interactions/Questionnaires

Generically, questionnaires are used to collect relevant information, usually applied to managers and system administrators. These questions are designed to ensure Pentest maximum efficacy and to provide a better understanding of clients' needs. The Pentester

should ask a great amount of questions or add optional ones (*see annex Ia – Pre-Engagement Interactions: Questionnaires*).

v. Pre-engagement Interactions/Establish lines of Communication

Establish lines of Communication for a quicker and efficient information transmission during Pentest, especially in case of emergency. A direct contact point should be pre-defined for eventual system failures.

vi. Pre-engagement Interactions/Rules of Engagement

The established engagement rules will allow to maintain Pentest conditions and its integrity. They should include Pentest methods, permissions, schedules, locations, execution times, and all legal considerations to protect the Pentester and its activities.

vii. Pre-engagement Interactions/Capabilities & Technology in place

Assess the organization responsiveness capability and its incident monitoring ability. The Pentester should perform the Pentest without conflicting with the technical team.

2.1.1.2. Intelligence Gathering Phase

Relevant data and information are collected to enable the recognition of a specific target, – building an image of the target – exposing its capabilities and vulnerabilities. From an offensive perspective, gathering information will allow a better understanding of how an attack can occur. For instance, through certain tools available in Open Source it is possible to find information about the device operating system, and if it is out of date. From a defensive perspective, the Pentester can assess existing vulnerabilities and implement preventive measures. The collection of information on organizations varies according to its organizational structure, its critical business assets and processes, partners and suppliers, financial information and others. The PTES recommends five tasks within this phase (*see annex II – PTES: Intelligence Gathering*):

i. Intelligence Gathering/Target Selection

Depending on the Pentest pre-determined scope, the target may or may not be identified.

When the target system information is known, Pentest is classified as “white box”. When there is no information it is classified as “black box”, which is an equivalent of a hacking attack. At this stage, the Pentester should confirm the established rules in the Pre-Engagement phase to check the test goals and the time available to perform it.

ii. Intelligence Gathering/OSINT

This section includes the Open Source Intelligence (OSINT), which is a form of Intelligence collection based on publicly available sources (**Nickerson et al., n.d.; OSINT FMI 2-22.9, 2006).** PTES recommendation has three forms of Intelligence Gathering: Passive, Semi-Passive, and Active.

OSINT collection can focus on physical, logical aspects – such as business partners, competitors, product line, vertical market, organization events, Internet suppliers – critical infrastructure and financial aspects of organizations. It can also focus on the individual, by searching for personal information that will sketch the relational profile.

iii. Intelligence Gathering/Covert Gathering

In this section are used less conventional activities to gather information about the target. These activities are frequently associated with dumpster diving and with the use of HUMINT techniques to collect information through a physical or verbal interaction. In these situations, there is a direct interaction with the target, using false identification to obtain relevant information, such as key employees, partners/suppliers, among others. It is also considered a phase with direct observation of information about wireless, radio signal frequencies, physical security mechanisms and physical accesses.

iv. Intelligence Gathering/Footprinting

This technique consists in a physical interaction with the target to obtain both external and internal information about the organization. The External Footprinting includes the identification of hosts and systems, using different techniques, such as reverse DNS, brute force, port scanning, WHOIS searches, domain research and others. The Internal Footprinting occurs when the Pentester has access to the internal network and is able to analyze the packet sniffing and extracting a variety of information, such as credentials from unencrypted Login Session's.

v. Intelligence Gathering/Identify Protection Mechanisms

Normally, organizations have certain protection mechanisms, such as firewalls and antivirus. Because these mechanisms can trigger alarms, it is mandatory to do a previous identification to maximize Pentest efficacy and minimize the detection ratio.

2.1.1.3. Threat Modeling Phase

Threat Modelling characterizes threats – threat agents and its capabilities – and allows to understand how a successful attack impacts on the organization and on its assets. PTES recommendation does not use a specific model, but recommends the use of a logical model in terms of its representation of threats and its impact. This phase has two key perspectives: (1) attacker, and (2) critical assets. The attacker perspective settles in the identification of relevant threats, threats agents and their capabilities. The critical assets perspective aims to identify all assets, whether are physical, logical, processes, humans or other. PTES recommends six tasks to understand this phase (*see annex III – PTES: Threat Modeling*):

i. Threat Modeling/Business Asset Analysis

For assets that are most likely to be attacked should be identified whether they are tangible or not. Such identification is possible through interviews and document analysis, collected in the previous phase.

ii. Threat Modeling/Business Process Analysis

Business models works through different sets of operating processes. In this task, it is essential to identify and list these processes, classify them as critical or non-critical, and identify its flaws. This allows to understand which processes, if exploited, could be harmful to the organization.

iii. Threat Modeling/Threat Agents & Community Analysis

The Pentester should identify and characterize potential threat agents, and consider if they are internal or external to the organization (*see annex IV – Threat Modeling: Threat Agents/Community Analysis*).

iv. Threat Modeling/Threat Capability Analysis

The estimation of the probability of a successful attack depends on the threat agents' capabilities. This task provides an understanding about the expertise the threat agent should have to exploit effectively critical assets.

v. Threat Modeling/Motivation Modeling

Threat agents' motivation should be identified and deeply analyzed. Depending on the organization, or even the market *status quo*, motivations can frequently change. Typical motivations are: curiosity, fun, challenge, reputation, competitiveness, profits and other benefits (direct or indirect), relationship matters – such as love problems (jealous and betrayal leads to passwords thefts, social profile and email intrusion) or partners surveillance – hacktivism, terrorism or even cyberwar.

vi. Threat Modeling/Finding Relevant News of Comparable Organizations

The Pentester should investigate about relevant past incidents or news related to organizations from the same business sector, and with parallel technological infrastructure. This knowledge, gained through historical analysis, such as challenges they have faced, can be often used as an indicator, helping to mitigate real incidents.

2.2. Intelligence

From a historical and institutional perspective, the word "Intelligence" has been used to designate secret governmental organizations and its activities. However, this concept has not been unanimous. Attempts to standardize this concept instigated several discussions and interpretations, which mainly settles on different political, cultural or temporal perspectives. In 2002, Michael Warner, CIA specialist, tried to gather different perspectives, classifying Intelligence in two categories: official and academic. On the one hand, official definitions are those registered in official documents or mentioned in laws (**Warner, 2002**). For instance, the National Security Department of the USA states in their record from 1947 that Intelligence (in particular, Foreign Intelligence) is "*information about the capabilities, intentions or activities of foreign governments, as well as their elements, organizations and foreign people*" (**National Security Act, 1947**). Another perspective is written in Joint Chiefs of Staff dictionary that perceives Intelligence in two different perspectives: *(1) "as a product, resulted from the collection, processing, integration, analysis and interpretation of available data and information about foreign areas or countries"*; and *(2) "as information and acknowledgement about a certain adversary, obtained through observation, investigation and analysis"* **(JP 1.02, 2001**).

On the other hand, academic perspectives refer to the commercial publications written by former specialists from Intelligence agencies, such as CIA. For instance, Sherman Kent published in 1949 the book "*Strategic Intelligence for American Foreign Policy*", on which Intelligence is defined as "*the acknowledgement that the individuals with senior positions in military should have to guarantee the National Security and well-being*" (**Kent, 1949**). About ten years later, in 1958, Mr. Random, also from CIA, wrote on his paper "*Intelligence as a Science*" that Intelligence is "*the collection and the processing of official or secret information about foreign countries to help to formulate and implement external policies and to lead secret activities on the outside to easier implement external politic*" (**Random, 1958**). Then, twenty years later, in 1978, CIA former director Veron Walter, wrote another definition for Intelligence: "*information which aren't always available in the public domain, related to force, resources, capabilities and the intentions of a foreign country, which may eventually affect our lives and the safety of our people*" (**Walters, 1978**).

After analyzing all these perspectives, we noticed that most of them focus on Intelligence as a product, recognizing it as a process. Therefore, these definitions neglect counter-

Intelligence and confine this concept to military and secret governmental organizations (**Bimfort, 1958**).

Across the years, political, cultural and even technological changes fostered the need to adapt and extend this concept to other domains. Even that Intelligence is mostly quoted into Law Enforcement domain, its definition is wider. The international Association of Chiefs of Police, in 2002, reported on "Criminal Intelligence Sharing" that Intelligence "*is the combination of credible information with quality analysis—information that has been evaluated and from which conclusions have been drawn"*(**IACP, 2002**). In 2010, UNODC publications about "Criminal intelligence" suggest a mathematical formula to understand Intelligence concept: "*Information + Evaluation = Intelligence*", where "*Information is simply raw data of any type, whilst in contrast Intelligence is data which has been worked on, given added value or significance*" (**UNODC, 2010**).

The most recent Portuguese perspective is offered by SIRP that sees intelligence "*as product that results from a process: information cycle*". Thus, it contemplates "*the data/facts/information collection through human ways, documental and technological and their organization, analysis and assessment through proper techniques and methodologies*". SIRP refers that "*information is an essential support tool when making political decisions, contributing to the safety, safeguard and national interest defense*" (**SIRP, 2017**).

Intelligence activity is typically associated to espionage and to the use of unconventional and illegal techniques and methods to obtain certain types of information. However, we consider that Intelligence *know-how* should be extended and applied to a large variety of domains, such as business, medical, academic sectors, among others, avoiding illegal approaches during the Intelligence process.

The following sections allows to understand the Intelligence foundations, highlighting its characteristics, conceptual evolutions and clarifying each phase of its cycle.

2.2.1. Data and Information

Data is defined as attributes obtained through specific sensors, observation, experimentation or calculation. Data is considered a set of values or occurrences with the lowest class of abstraction, this is, data has no significance when isolated (**Bergeron, 2003; Goldman, 2006**). Conversely, information is understood as the explanation and interpretation of raw data. It has a higher abstraction class, that is, information is created when data is contextualized, gaining a specific meaning (**Bergeron, 2003).** For instance, if we consider

isolatedly each variable, "150", "Massive spread", "98%" and "may", we can't attribute them a specific meaning, as represented in "*Figure 1 – Raw Data"*.

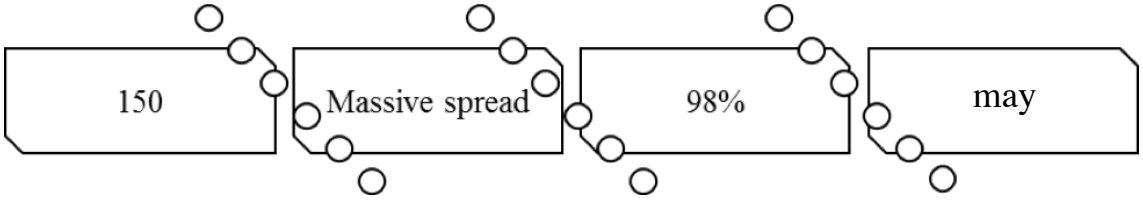

Figure 1 – Raw Data

However, when we look to the same raw data but within a specific context, for instance "Cyber-attacks", they gain a different interpretation.

We developed a simple exercise consisting in searching on Google for "*150 massive spread 98% may*". We found over 500 000 random results, which turns data interpretation very complex or even impossible. Then, we simply added the context "Cyber-attack", searching now for "Cyber-attack 150 massive spread 98% may". It was impressive that the top 10 results reported the same: a massive ransomware (WannaCry) attack spread, occurred in 12th May 2017 that affected over 150 countries. It could spread through computers running unpatched versions of Microsoft Window. About 98% of the affected devices had some version of Windows[1].

The "*Figure 2 – Contextualized Data*" illustrates the difference after attributing a specific context to raw data.

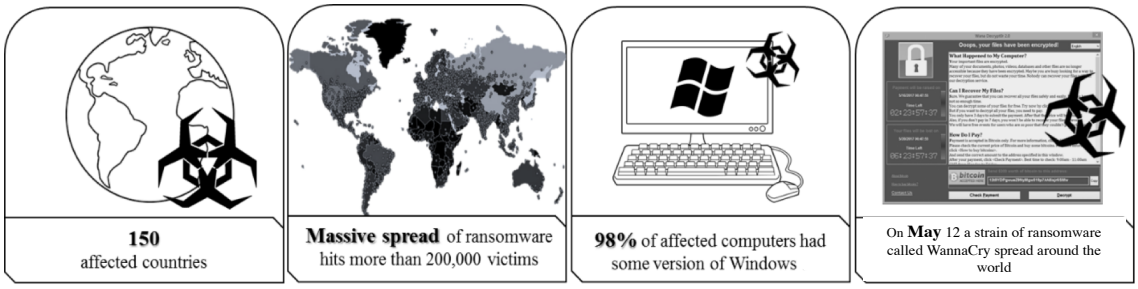

Figure 2 – Contextualized Data

In conclusion, raw data cannot speak by itself, its meaning depends on the situation on which is interpreted. We also realized that it is possible to analyze different attributes and withdraw empirical correlations between things that apparently are not connected.

[1] Attack confirmed by Europol. Available: <https://www.europol.europa.eu/wannacry-ransomware>. [June, 2017].

2.2.2. Intelligence Characterization

Intelligence can be characterized in two different perspectives: as an activity and as a result (**Kent, 1949; Random, 1958; Bimfort, 1958; Walters, 1978; Krizan, 1999; Warner, 2002; Schulsky & Schmitt, 2002; Goldman, 2006**; **Lowenthal, 2008; Khan, 2009; McDowell, 2009)**. As an activity, it is defined as "*production and use of information carefully analyzed and adapted for specific users* (**Krizan, 1999**)". As a result, it is considered a "*final product derived from a process whose response materialize in many levels and replies to the specific needs of the decision-maker* (**Goldman, 2006**)".

Intelligence products are placed in one of nine production categories: warning, target, current, prospective, general military, basic research, scientific and technical (S&T), identity intelligence (I2) and Counterintelligence (CI) (**Johnson, 2007; JP 2-0, 2013**) (*see Figure 3 - Intelligence Products*):

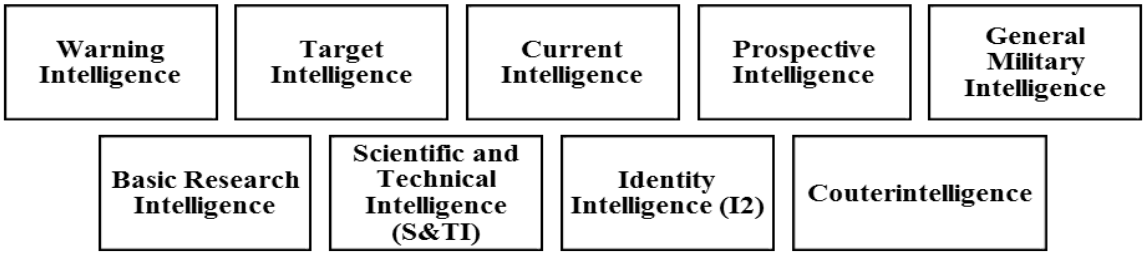

Figure 3 – Intelligence Products[2]

The same intelligence and information can be used in each category. However, the categories are distinguished mainly by the purpose for which the Intelligence was produced, as described as follows:

1. Warning Intelligence

It has the purpose of providing warnings to anticipate hostile activities and assessing the occurrence probability of those activities (risk evaluation). It has an urgency and a time sensitive nature otherwise it will lose its value (**Goldman, 2006; Grabo, 2010; JP 2-0, 2013)**.

2. Target Intelligence

It has the purpose of providing portraying and locating the components of a target or complex target, such as networks and support infrastructures, indicating its vulnerabilities and relative importance. Includes physical, moving or virtual targets analysis (biographic, biologic,

[2] Note: Adapted from **Johnson (2007)**, **JP 2-0 (2013**).

behavioral, and reputational attributes of human targets) and signature (detection and positive identification of targets). Target intelligence must holistically analyze the target, so it also includes functional systems vulnerabilities' and damage capabilities (**JP 3-60, 2013; CJCSI 3370.01, 2016**).

3. Current Intelligence

It has the purpose of providing updated support for ongoing operation. It involves producing and delivering Intelligence about an existing incident. It also involves the integration of time-sensitive and all-source intelligence, identifying and evaluation risks (**Hedley, 2007; JP 2-0, 2013**). It aims to identify adversary's capabilities, intentions, vulnerabilities, assets and other interesting activities (**Goldman, 2006**).

4. Prospective Intelligence

It has the purpose of forecasting incidents with a three to five years strategic orientation about new politics and decision-making development (**Johnson, 2007**). It includes a description of relevant actors' capabilities and activities estimating potential consequences. It includes the production of alternative scenarios to support the best strategic decision (**Hedley, 2007**).

5. General Military Intelligence (GMI)

It has the purpose of monitoring military capabilities, identifying forces and dispositions of foreign countries, organizations and non-state actors that are potential threats to the military operations and/or national security. This category is usually associated with long-term planning and attempts to identify and monitor trends, including the identification of strengths and weaknesses, technical capabilities and infrastructure characteristics **(JP 2-01, 2012).**

6. Basic Research Intelligence

It has the purpose of providing reference data such as biographical data, geographical, military, economics, social, demographic and political. Results are presented in monographies, maps, schemes, and summaries (**Johnson, 2007; Hedley, 2007**). It supports not only the Current Intelligence but also the Prospective Intelligence (**ITACG, 2011**).

7. Scientific and Technical Intelligence (S&TI)

It has the purpose of examining foreign scientific and technical (S&T) developments with warfare potential. It includes S&T characteristics, capabilities, vulnerabilities and limitations. It covers the spectrum of applied sciences and technologies, including tactics, equipment efficiency and its systems (**Johnson, 2007; JP 2-0, 2013**).

8. Identity Intelligence (I2)

It has the purpose of identifying links and patterns between agents that may be considered a threat. Results from the merge of identity attributes, such as biological characteristics, biographical, behavioral, reputational, relational related to individuals, and other information associated with those attributes. For this correlation, I2 uses Biometric-enable Intelligence (BEI), Forensics-enable Intelligence (FEI), and Documents and Media Exploitation (DOMEX) to discovery unknown threats (**JP 2-0, 2013).**

9. Counterintelligence (CI)

It has the purpose of gathering information to identify, deceive, exploit disruption, sabotage and any other activities of foreign entities that may be a threat. CI identifies weaknesses and vulnerabilities that may be exploited by an adversary, which can be used to implement security measures against foreign Intelligence (**JP 2-0, 2013; Cleave, 2015).**

2.2.3. New Intelligence Paradigm

Traditional Intelligence is comparable to puzzles where pieces are missing. Therefore, the goal is to gather as many pieces as possible to further analysis, using secret or publicly available pieces. Even if Intelligence keeps using traditional sources of classified information and methods, such as undercovered missions, it must devise ways to deal with the new challenge associated with the large amount of information available in open sources, which is consequence of the rapid technological evolution (**Lahneman, 2010**).

This evolution also has given rise to new threats and risks within a variety of areas supported by technological infrastructures, threatening security in several domains and in nontraditional ways. Therefore, it seems that considering a new intelligence paradigm is the only way to deal with modern times. The new paradigm is composed of trends which have recently appeared in Intelligence domain, making it harder for Intelligence Services to provide relevant information, such as: (i) the potential human rights encroachment and freedoms confines data-gathering by Intelligence Services; (ii) the requirement for intelligence and evidence with forensic value; (iii) the increased capacity for the transmission of large amounts of data and information through Internet, television and phone calls, makes Intelligence services unable to deal with this fast exchanging of news; (iv) the existing access and usability of information technology allows billions of people to use the Internet, but some may misuse it (**Črnčec, 2009**).

The following "*Table 2 – Intelligence Evolution*" offers a comparison between traditional Intelligence focus and its new perspectives.

TRADITIONAL INTELLIGENCE FOCUS	NEW INTELLIGENCE GOALS
Products	Outputs
Statistics & performance driven	Consumer needs-driven
Static production process	Analyst exchange during research/production process (incl. outsiders)
Static products	Dynamic and static outputs
Discrete	Discrete Share while protecting sources and methods
Inconsistent feedback/lacking effective feedback mechanisms	Effective and utilized feedback mechanisms
No defined audience	Clearly defined audience
Set scopes/purposes determined by producing agency	Evolving and shifting scopes to meet consumer requirements
Analysts as producer to policymaker/decision maker	Value-added producer to consumers who need the intelligence
Product disseminated and complete	Dialogue between producer and consumer before and during production
Finished Intelligence	Useful information and analysis to consumer
Traditional dissemination mechanisms	Traditional and non-traditional dissemination (incl. analysts as output via social media, etc.)

CONCEPTUAL EVOLUTION

Table 2 – Intelligence Evolution[3]

Over the years, Intelligence (military concept) has its focus on the development of the process behind products production, neglecting the customers' needs. Nonmilitary threats are increasing in relation to military ones, requiring Intelligence to be adapted to different needs. In addition, the above-mentioned trends required an emerging change which led to open the restricted military Intelligence concept to non-military environments, such as the business sector. Finished Intelligence was always seen as a static Product, however, the new trend such as the Internet and social media networks, provided openings for rethinking this concept, changing it to dynamic outputs (constantly updating and disseminating information around the world). The new Intelligence paradigm focuses on consumer needs and encourages dynamic processes, such as knowledge sharing and feedback mechanisms between producers and consumers. It also has a well-defined audience, scope and terms, contemplating consumers' needs. Even if supporting these needs leads to a more complex work, when compared to delivering a single product, the output (final result) is value-added

[3] Note: adapted from **Lahneman, W.J. 2010; Analyst-IC Associate Teams Program (2012**)

to support consumer decisions (**Lahneman, W.J. 2010; Analyst-IC Associate Teams Program, 2012**).

2.2.4. Traditional Intelligence Cycle

The Intelligence process is traditionally represented by the Intelligence Cycle consisting of five phases: 1. Planning; 2. Collection; 3. Processing; 4. Analysis and Production; 5. Feedback & Dissemination; as represented in "*Figure 4 – Traditional Intelligence Cycle"*.

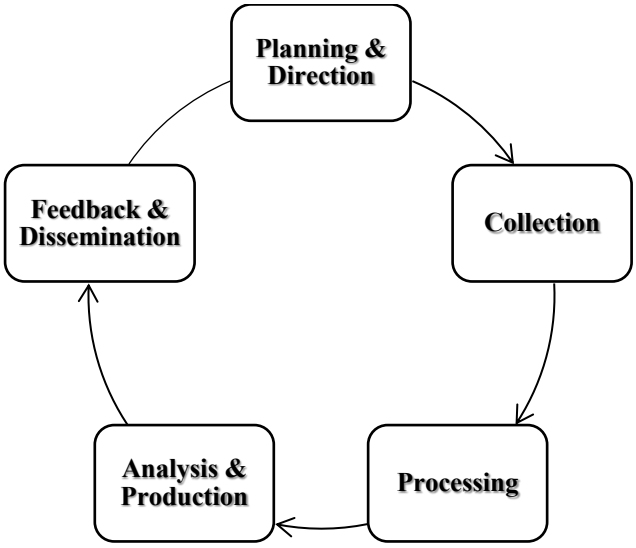

Figure 4 – Traditional Intelligence Cycle[4]

The Intelligence cycle is the process of transforming raw information into finished Intelligence. It can be restarted if the final output does not match with the requirements defined in the first phase. All phases ensure that the process flows correctly thought an auditable system of checks and balances. In the next sections we describe each phase (**Krizan, 1999; Goldman, 2006; Studies in Intelligence, 2012; CIA, 2013, JP 2-0, 2013; Fiães, 2014; Omand, 2014**):

i. Phase 1 – Planning & Direction

In this phase Intelligence needs are identified and transformed into Priority Intelligence Requirements (PIR) that are high priority information, and into Other Information Requirements (OIR) that are minor priority information. For each PIR/OIR a set of questions (5W2H), such as "*What? Who? Where? Why? When? How? How much?*", should be answered in order to identify what is known and unknown (*see Figure 5 – Intelligence*

[4] Note: adapted from **Krizan, 1999; Goldman, 2006**; **Studies in Intelligence, 2012; CIA, 2013; JP 2-0, 2013.**

Needs). This phase is seen as the macro management of the entire Intelligence cycle activities. Therefore, should be created a research plan to identify which questions should be researched to answer to PIR/OIR, identify sources of information, and identify means and forms of information gathering. This plan also outlines all needed resources; defines the useful time-life of information, allowing Intelligence to be targeted, precise and timely; and follows the entire Intelligence process as a chain of custody (**Goldman, 2006; ITACG, 2011; CJCSM 3314.01A, 2012; JP 2-0, 2013; Fiães, 2014**).

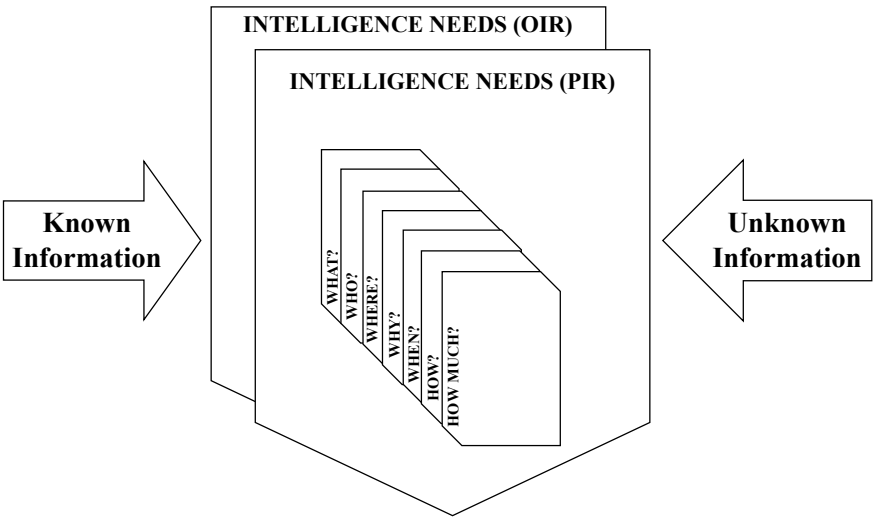

Figure 5 – Intelligence Needs[5]

ii. Phase 2 – Collection

This phase is characterized by a dynamic and continuous process of research and collection of raw data to satisfy the requirements specified in the Planning & Direction phase. This phase is managed through a Collection Plan (dynamic plan), that has the objective of selecting the most appropriate sources of data collection to satisfy with effectiveness the Intelligence needs. When adjustments to the Collection Plan are made, analysts must inform their supervisors. It is also on this phase that Information is classified according to type (private or public) and source (confidential or open) (*see annex VI – Information Classification*) (**Goldman, 2006; FMI 2-22.9, 2006**). Intelligence can also be characterized according to means of collection: Human collection and Technological collection, as represented in the diagram "*Figure 6 - Intelligence Collection Source*".

[5] Note: adapted from **Fiães, 2014.**

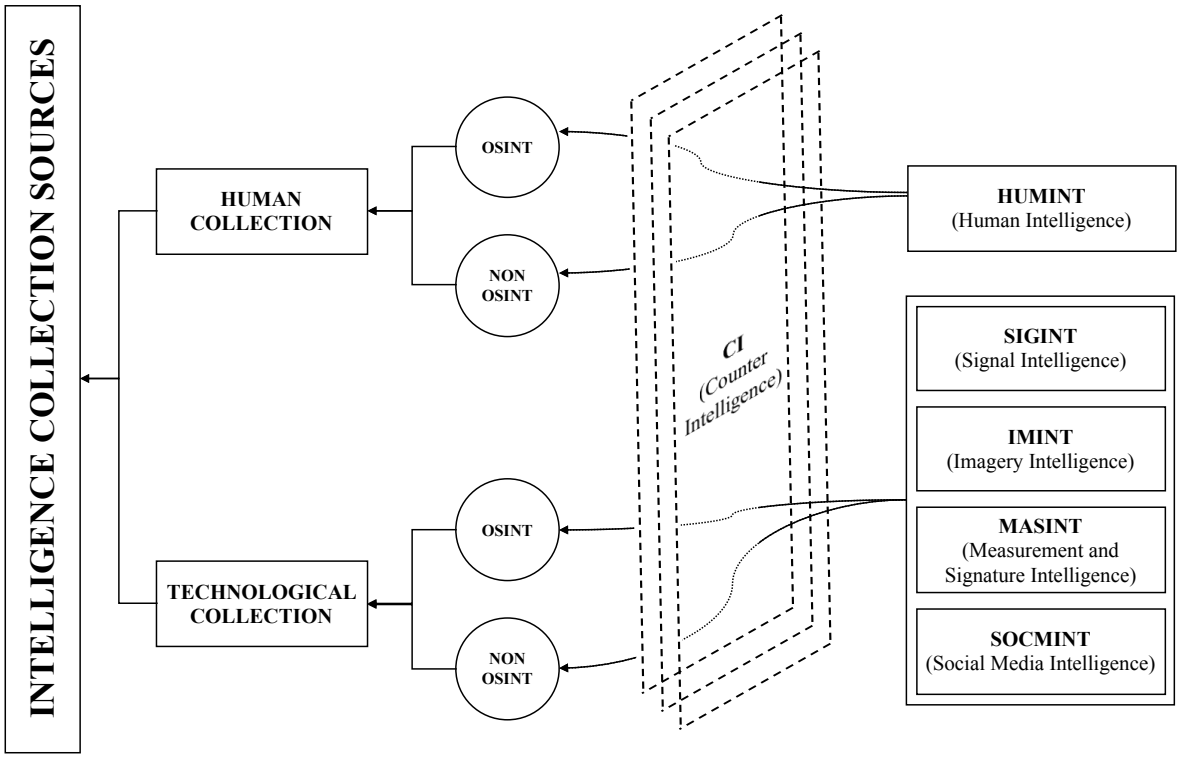

Figure 6 – Intelligence Collection Source

Human collection consists in the collection of data and information through human sources, i.e. a human element is used as source of Intelligence through direct, incentive or emotional approaches using deception techniques such as interviewing (debriefings or interrogations) and elicitation (**FM 2-22.3, 2006, West 2006, Hitz, 2007**). Technological collection consists in the collection of data and information through technological sources, i.e. technological elements that are used as source of Intelligence, which can be classified as Signals Intelligence (SIGINT); Imagery Intelligence (IMINT); Measurements and Signatures Intelligence (MASINT) and Social Media Intelligence (SOCMINT) **(Richelson, 2007; George et al., 2008**; **Omand et al., 2012).** Both, Human collection and Technological collection, can be used to apply Counterintelligence (CI). CI refers to information and activities conduced to protect against other Intelligence services, such as espionage, manipulation or sabotage operations, and can be seen in three perspectives: (1) collective; (2) defensive; and (3) offensive. The first consists in gathering information about the adversary Intelligence collection capabilities. The second refers to conducting countermeasures to mitigate hostile penetration activities. And the third consists on manipulating adversary Intelligence with false information or turning its agents in double agents **(West, 2006, JP 2-0, 2013, Cleave, 2015).**

Lastly, all investigations begin with data that is available openly (OSINT data) and with data that is not (Non-OSINT data). Open Source Intelligence (OSINT) is defined as legal collection of data and information that can be accessed without special authorization or associations. Such type of data may be Geographical Data (postcodes, street names); Statistical Data; Electoral Register; Court Records; Social Media; Blogging Platforms; Search Engines; Internet Archive; Freedom of Information[6](**NATO, 2001; Gibson, 2004; Lowenthal, 2006; Graça, 2010**; **Day, et al., 2016**). Non-OSINT Data refers to data that has not been made publicly available, due to being under a proprietary/company or restricted license, such as Criminal Records, Financial Records, Telecommunication Records, Medical Records, Imagery, Sensors and Video Data (**Omand et al., 2012; Day, et al., 2016**). It is also on this phase that gathered data and information are subjected to an evaluation, ensuring its consistency, usefulness and confidence through evaluations matrices (*see annex VII – Evaluation Matrix*).

iii. Phase 3 – Processing

This phase consists in processing raw collected data and converting it into a usable and organized format. Typically, the Collection phase produces large amounts of unfiltered data that should be converted into an eligible form. The Processing phase includes signal decryption, imagery exploitation, documents and media translation and decoding, data conversion and correlation. It prepares raw data entry to database processing (**Goldman, 2006; JP 2.0, 2013; JP 1-02, 2016)**.

iv. Phase 4 – Analysis & Production

During this phase Intelligence is produced from the information gathered by the Collection phase. All processed information goes through a process of integration, evaluation, analysis and interpretation to create products (*see Figure 3 – Intelligence Products Taxonomy*) that will satisfy PIRs. This phase has two steps: (1) analysis, and (2) production. The first, *Analysis*, consists in the integration of available data into a context, producing value-added information to the consumer (**Goldman, 2006; Mangio & Wilkinson, 2008; JP 2.0, 2013).** Analysis step allows to establish links and assign meanings. It is supported by Structured Analytical Techniques (SAT) which helps to externalize internal processes in a systematic

[6] Freedom of Information is related to the public having access to information held by governmental organizations (**Day, et al. 2016**).

and transparent way (*see section 2.2.5. Structured Analytic Techniques*). Each SAT leaves a trail allowing others analysts to follow and see the foundation of an analytic judgment, avoiding as well cognitive biases and intuitive traps (**Heuer & Pherson, 2011**). The second, *Production*, consists in the preparation of the results that can be presented in reports, briefings, and estimates (**Goldman, 2006, JP 2.0, 2013**). A proper language should be used to estimate probability of occurrence or links between events and to assess hypotheses degrees of confidence (*see annex VIII – Qualitative Language*).

v. Phase 5 – Feedback & Dissemination

Feedback consists in a dialog between Intelligence producers and consumers that should continuously occur before and after Intelligence is delivered. The feedback mechanism is useful to assess if the finished Intelligence meets the initial needs of Intelligence and to report required adjustments (if there are inconsistencies, Intelligence cycle should be restarted). Intelligence processes ends with Dissemination. This process consists in the diffusion of the finished Intelligence to who requested the Intelligence, that is, when it reaches the decision makers. Those who are responsible for Intelligence dissemination must guarantee the integrity, confidentiality and authenticity of all activities during the process (**Goldman, 2006; Lowenthal, 2008**).

2.2.5. Structured Analytic Techniques

There are four main methods used in Intelligence analysis: (1) quantitative methods using empirical data, (2) quantitative methods using expert-generated data, (3) expert judgments, and (4) structured analysis, which are represented in "*Figure 7 – Intelligence Analytical Techniques*" (**Clark, 2007; Heuer & Pherson, 2011)**.

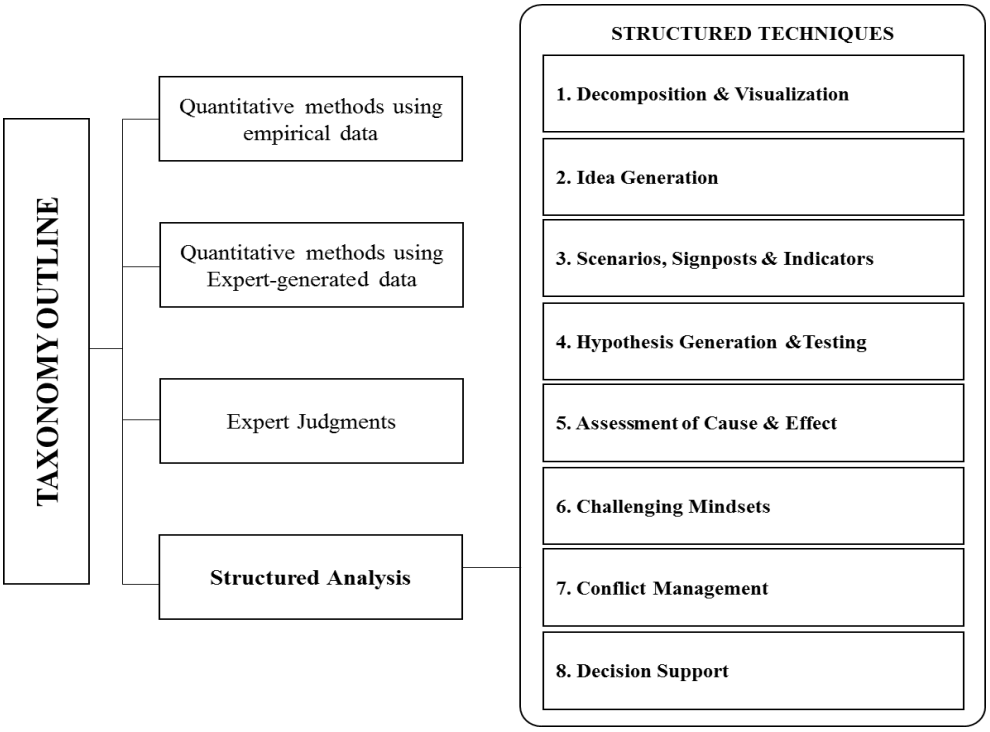

Figure 7 – Intelligence Analytical Techniques[7]

None of these methods is preferential, they are all necessary to optimize chances to find adequate results. The best practice is to use multiple methods to get accurate results.

Quantitative methods using empirical data consist in the use of collected data from any type of sensors, i.e. network traffic analysis (which allows to identify the sources and destinies of traffic, or even packets numbers to detect DDoS attacks). Conversely, quantitative methods using expert-generated data consist in evaluations obtained through decision analysis, Bayesian inferences, dynamic models and simulations. Moreover, expert judgment which is also known as intuitive analysis, refers to expert opinions based on evidence reasoning, critical thinking, historical analysis, case study analysis and reasoning by analogy. There are also structured techniques (SAT) that helps to reduce the adverse effects that may result from experts' cognitive limitations and manipulations. These techniques consist in the externalization and decomposition of thinking, in such a methodical way that it can be

[7] Note: adapted from **Heuer & Pherson, 2011**

reviewed and criticized step by step by other experts (**Lefebre, 2004; Heuer & Pherson, 2011**). SAT has eight categories, each one with a specific purpose, as explained following:

1. **Decomposition & Visualization**

The large amount of data and information to be analyzed is often a limitation because most people only have the capacity to keep in the working memory about seven (plus two or less two) things at the same time. As the complexity increases also the number of variables increases, so it is very difficult to conduct analysis without errors only based on our head. There are two approaches for dealing with such complexity: (1) Decomposition, which divide things into components in order to deal with each part separately; (2) Visualization, which place the divided parts on paper or on computer in an organized way, such as lists, matrices, maps, trees, in order to visualize the existing relations;

2. **Idea Generation**

It has the purpose of encouraging the creation of new ideas, allowing to broaden the horizons to different perspectives and premises. Combining old ideas with new perspectives is essential. However, generating new ideas or producing divergent ideas is more effective in group than individually. Techniques such as brainstorming, quadrant crunching, general morphological analysis and cross-impact matrix are really useful to identify different perspectives and stimulation new ideas.

3. **Scenarios, Signposts & Indicators**

The human mind tends to see the expected and to ignore the unpredictable. Some events are not easily predicable and the best approach to determine future outcomes is Scenario Analysis. Generating alternative scenarios provides a set of outlined options with value added for the decision maker. Including impact/low probability scenarios, such as signposts and indicators, is useful to delivery early warnings about significant changes. These changes sometimes are so gradual that we do not perceive it, or consider it pertinent. Therefore, the identification of indicators, flags and scenarios allows the creation of efficient mechanisms for rationalization.

4. **Hypothesis Generation & Testing**

The most common cause of Intelligence flaws lays on bounded mental models and intuitive judgments. Generation and testing hypotheses process is a core element of Intelligence analysis and it is supported by the collection and presentation of evidences. This process requires two parts: the first part describes techniques to formulate and

categorize hypotheses, such as Simple Hypotheses, Multiple Hypotheses Generator, Quadrant Hypothesis; the second part describes techniques to test hypothesis, such as Diagnostic Reasoning, Analysis of Competing Hypotheses, Argument Mapping, Deception Detection.

5. Assessment of Cause & Effect

Attempts to explain the past or the future having as basis the understanding of a root cause and its effect. This understanding gets difficult when variables and relationships in study have no theory behind or are unpredictable, such as the human behavior. This analysis is tendentially conditioned by the analyst perception and experience. Techniques such as Key Assumptions Check, Structured Analogies, Role Playing, Red Hat Analysis, Outside-In Thinking, Policy Outcomes Forecasting Model and Prediction Markets are useful to mitigate cognitive pitfalls involved in analysts' judgments.

6. Challenging Mindset

It has the purpose of challenging established mental models, broadening minds to other possible explanations. The analytic mental model (mindset) is a key factor for the failure because when external conditions change the mental model usually does not follow the change. For instance, mental models which have been provided truthful assessments and estimations for years are resistant to changing mindsets. Techniques such as the Premortem Analysis, Delphi method, What if? Analysis, High Impact/Low Probability Analysis, Red Team Analysis and Devil's Advocacy, are great techniques to mitigate preconceived mental models, exposing diverse perspectives on a certain subject or evidence;

7. Conflict Management

It has the purpose of managing different mindsets that usually leads to confrontation of views to become instead a grow learning experience. Conflict Management techniques should also be used when there is a high degree of uncertainty about a certain point of view. Techniques such as Key assumptions check, the Nosenko approach, Argument mapping and Joint escalation, are really useful when dealing with analytical conflicts;

8. Decision Support

Given the limitations of human short-term memory, it is easy to forget all pros and cons when we have simultaneous options. The focus will be on one option at each time which leads to fragile decisions. Techniques such as SWOT Analysis, Decision Matrices, Force

Field Analysis and Pros-Cons-Faults- and-Fixes (PCFF), places all the options and their relationships in graphical format which helps to overcome this cognitive limitation.

Each of the previous referred categories has specific techniques (see *Figure 8 – Structured Analytic Techniques*) that can be used to deal with an extensive variety of subjects. The challenging task is knowing how to select the right technique to apply on a particular scenario. However, there has been made a remarkable effort in grouping these techniques considering specific scenarios (see *Figure 9 – Selecting the right technique*) (**Heuer & Pearson, 2011**).

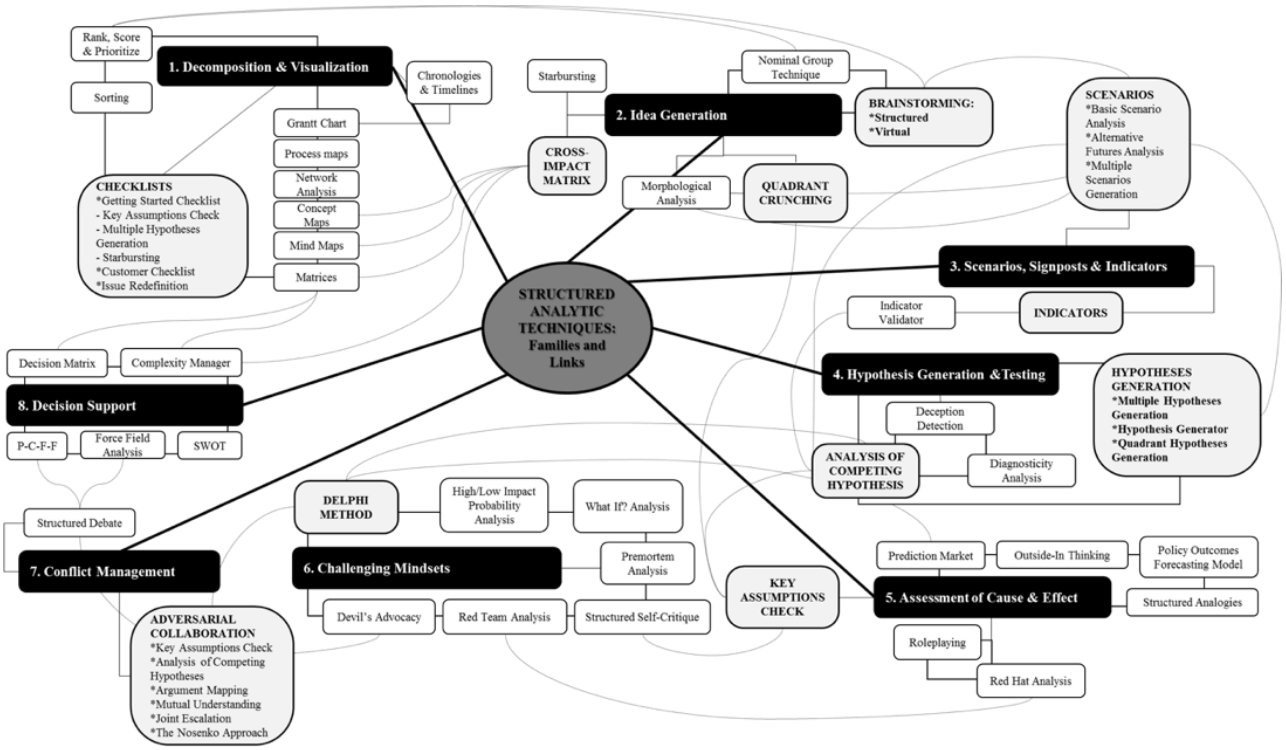

Figure 8 – Structured Analytic Techniques[8]

SELECTING THE RIGHT TECHNIQUES

❑ Define the project?

1. Decomposition & Visualization
   - **Checklists; Issue Redefinition**
2. Idea Generation

❑ Get Started? Generate a list (e.g. driving forces, variables to be considered, indicators, important players, historical precedents, source of information, or questions to be answered? Organize, rank, score or prioritize the list?

1. Decomposition & Visualization
2. Idea Generation

❑ Examine and make sense of the data? Figure out what is going on?

1. Decomposition & Visualization
   - **Chronologies and Timelines; Sorting; Network Analysis; Mind Maps & Concept Maps**
2. Idea Generation
   - **Cross-impact Matrix**

❑ Explain a recent event; assess the most likely outcome of an evolving situation?

4. Hypothesis Generation &Testing
5. Assessment of Cause & Effect
6. Challenging Mindsets

❑ Monitor a situation to gain early warning of events or chances that may affect critical interests? Avoid surprise?

3. Scenarios, Signposts & Indicators
6. Challenging Mindsets

❑ Generate and test hypotheses?

4. Hypothesis Generation &Testing
5. Assessment of Cause & Effect
   - **Key Assumptions Check**

❑ Assess the possibility of deception?

4. Hypothesis Generation &Testing
   - **Analysis of Competing Hypotheses; Deception Detection**
5. Assessment of Cause & Effect
   - **Key Assumptions Check; Role Playing; Red Hat Analysis**

❑ Foresee the future?

3. Scenarios, Signposts & Indicators
4. Hypothesis Generation &Testing
   - **Analysis of Competing Hypotheses**
5. Assessment of Cause & Effect
   - **Key Assumptions Check; Structured Analogies**
6. Challenging Mindsets
8. Decision Support
   - **Complexity manager**

❑ Challenge your own mental model?

6. Challenging Mindsets
2. Idea Generation
4. Hypothesis Generation &Testing
   - **Diagnostic Reasoning; Analysis of Competing hypotheses**
5. Assessment of Cause & Effect
   - **Key Assumptions Check**

❑ See events from the perspective of the adversary or other players?

5. Assessment of Cause & Effect
   - **Key Assumptions Check; Role Playing; red Hat Analysis**
6. Challenging Mindsets
   - **Red team Analysis; Delphi Method**
7. Conflict Management

❑ Manage conflicting mental models or opinions?

7. Conflict Management
4. Hypothesis Generation &Testing
   - **Analysis of Competing Hypotheses; Argument Mapping**
5. Assessment of Cause & Effect
   - **Key Assumptions Check**

❑ Support a manager, commander, action officer, planner, or policy maker in deciding between alternative course of action; draw actionable conclusions?

8. Decision Support
7. Conflict Management
4. Hypothesis Generation &Testing
   - **Analysis of Competing Hypotheses**

Figure 9 – Selecting the right techniques[8]

[8] Note. **Heuer & Pherson, 2011.**

3. iPENTEST PROPOSAL

This chapter begins with the explanation of iPentest methodology, which offers an improvement proposal for PTES Pre-Engagement Interactions and Threat Modeling phase. iPentest proposal brings two value added innovations for the execution of Pentests and for the scientific community: the first iPentest methodology highlight relies on the improvement of Pre-Engagement Interactions phase, henceforth named Planning & iScenario phase. To this phase we added a structured thinking toolkit which increases the Pentesting planning efficiency. We also proposed a methodology that offers the possibility to execute the Pentesting directing it to specific scenarios (iScenario); the second highlight relies on the Threat Modeling phase where we proposed a solution to fill the existing gap from PTES Threat Modeling phase. This solution, henceforth named iModeling Universe of attributes, can be applied on three different contexts: (1) Penetration testing mapping; (2) Cybercriminal investigation; (3) Cyber risk analysis.

(1) Penetration testing mapping: this approach is based on Penetration testing mapping for current or prospective security status assessment. It can be used for both, defensive (Pentester) and offensive (hacker) perspectives;

(2) Cybercriminal investigation: this approach is based on criminal cyber incident mapping. It can be used for criminal investigation analysis in that it allows the identification of potential criminal root causes and the creation of cyber-crime profiling;

(3) Cyber risk analysis: this approach is based on Cyber risk analysis, determining the impact of business assets and processes within the organization. It can be used for several purposes such as Information Security Assessment, General Data Protection Regulation (EU) 2016/679 (GDPR) compliance, or Cyber insurance assessment.

3.1. Methodology

The Pentest begins with the pre-engagement phase, which involves talking with customers and evaluating their needs and expectations. It is possible to gather great information about customer's organization and infrastructure even before interacting with the technological infrastructure. However, gathering correct information is a hard task to complete, particularly when the plan is not properly prepared. Therefore, we considered urgent to design an approach that could help to improve Pentesting results. iPentest methodology was

created applying Intelligence techniques on both, Planning and Threat Modeling phase, as represented in the "*Figure 10 – iPentest methodology"*.

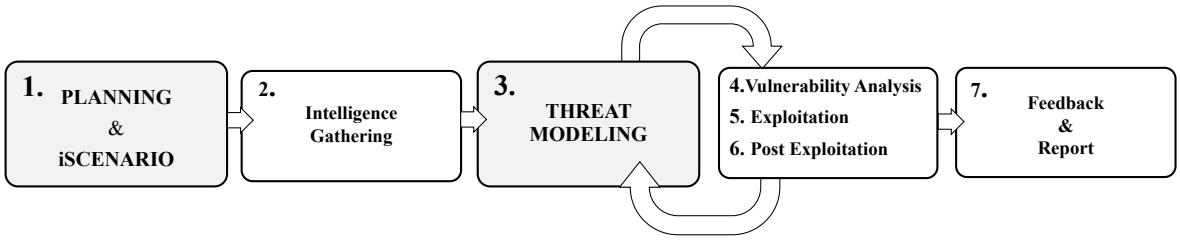

Figure 10 – iPentest Methodology

iPentest Methodology consists in the following seven phases: 1. Planning & iScenario; 2. Intelligence Gathering; 3. Threat Modeling; 4. Vulnerability Analysis; 5. Exploitation; 6. Post Exploitation; 7. Feedback & Report. This methodology offers the PTES recommendation a proposal improvement for the Pre-engagement Interaction phase and Threat Modeling phase, hereinafter referred as Planning and Threat Modeling phase. The advantage of both phases it's the integration of analytical Intelligence techniques contributing to more precise and efficient Pentesting. Each phase is explained in detail in the succeeding sections. Minor, but not less important, we propose a slight adjustment on PTES last phase (7. Report), which consists on adding a feedback mechanism between Pentester and Customers before the Report delivery.

3.1.1. Planning phase

The Planning phase aims to perceive customer's needs and to define the Pentesting scope (what is to be tested and how the Pentest will be conducted). This phase is indispensable to improve Pentesting results by aiding better focus and reducing scope ambiguity, as well to Pentesters coordination, control, resource and time management. Yet, the Planning phase continues to be frequently overlooked by Pentesters **(Nickerson et al., n.d).**

Therefore, our proposal for iPentest Planning phase offers Pentesters a reflection tool (structured thinking methodology) useful for processing customer's needs, which will guarantee time saving, increase research efficiency as well as the quality of Pentest results. Also, applying *Decomposition & Visualization* and *Idea Generation* techniques on the first phase of Pentests helps to anticipate Pentester actions and to develop specific observables about customer's needs.

iPentest Planning phase begins with two tasks: (i) Define iNeeds; (ii) Systematize iNeeds. The first task, designated Define iNeeds, consist in listening, reflecting and processing the

customer needs in a structured manner. It can be accomplished by using Questionnaires and then applying SAT such as *Getting Started Checklists*, *Customer Checklist* and *Issue redefinition* (**Heuer & Pearson, 2011**). The second task, designated by Systematize iNeeds, consists on creating a working plan that defines the major steps to reach the defined iNeeds and includes resource scheduling. It also serves as a communication tool between the Pentester and the customer, a high-level document that helps non-technical individuals to understand the Pentest. It can be accomplished by using SAT such as *Roadmaps*, *Chronologies & Timelines, Ranking-Scoring-Prioritizing, Matrices* and *Network Analysis* (**Heuer & Pearson, 2011**).

Another innovation for the first phase of iPentest methodology is the possibility the customer has to select specific Scenarios (iScenario) for the Pentest. iScenario options are place in one from eight categories: iCurrent, iWarning, iFuture, iDecision, iHypotheses, iDeception, iChallenge, iConflicting (see *Figure 11 – iPentest: Planning & iScenario*). This allows the Pentester to follow a methodology that will help him to focus the Pentest on the selected category. These categories are distinguished from each other's according to their purpose as described below:

1. **iCurrent**

It has the purpose of providing updated Intelligence about the current security status. Intelligence Gathering and consequently Reporting will be structured in a manner to return results about existing risks to Business assets and processes;

2. **iWarning**

It has the purpose of providing early warnings to anticipate hostile activities, avoiding unexpected surprises. Intelligence Gathering and consequently Reporting will be structured in a manner to assess the probability of these hostile actions to occur and its impact to Business assets and processes;

3. **iFuture**

It has the purpose of forecasting hostile incidents and trends. Intelligence Gathering and consequently Reporting will be structured in a manner to characterize relevant actors, its capabilities, threats and its consequences to Business assets and processes;

4. iDecision

It has the purpose of supporting business managers in deciding between alternative courses of action. Intelligence Gathering and consequently Reporting will be structured in a manner to decision support and includes the design actionable conclusions to Business assets and processes;

5. iHypotheses

It has the purpose of generating and testing alternative hypotheses. Intelligence Gathering and consequently Reporting will be structured in a manner to provide alternative scenarios related to Business assets and processes;

6. iDeception

It has the purpose of detecting deception. Intelligence Gathering and consequently Reporting will be structured in a manner to evaluate the possibility of deception to Business assets and processes and includes the design of a treatment plan to reduce deception;

7. iChallenge

It has the purpose of challenging existing mental models. Intelligence Gathering and consequently Reporting will be structured in a manner to challenge mindsets, generate new ideas and includes an assessment of cause effect to Business assets and processes;

8. iConflicting

It has the purpose of challenging conflicting mental models or opinions. Intelligence Gathering and consequently Reporting will be structured in a manner to design a plan to managing conflicts that may affect business assets and processes.

The previously mentioned scenarios are reached through the combination of different SAT (*Figure 12 – iPentest: Planning & iScenario SAT*) and vary according to its purposes. When dealing with complex problems it's recommended to use multiple techniques simultaneously. For instance, the customer is deeply concerned that unexpected surprises against its business assets and processes may occur, and decides to select iWarning scenario. Subsequently, the Pentester will gather and organize Information using "3. Scenarios, Signposts & Indicators" techniques, such as *Alternative Futures Analysis* and *Indicators,* and "6. Challenging Mindsets" techniques, such as *What If? Analysis*, *Devil's Advocacy*, *High/Low Impact Probability Analysis* and *Red Team Analysis* (**Heuer & Pearson, 2011**).

The Pentesting Report will highlight warnings about unexpected and hostile activities against Business assets and processes.

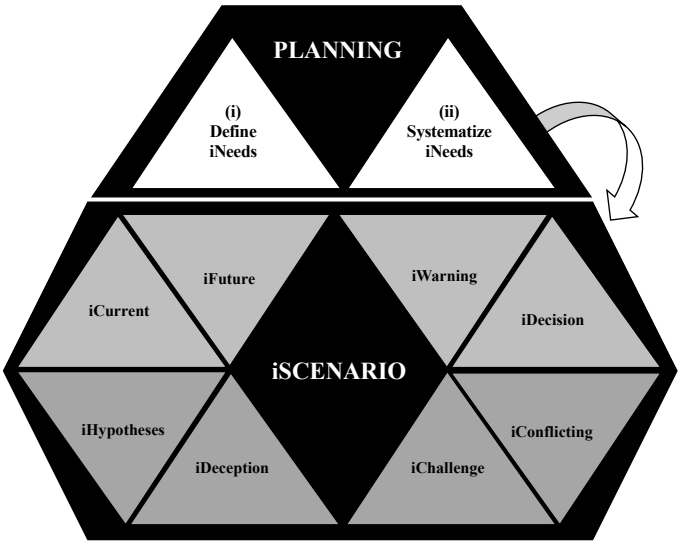

Figure 11 – iPentest: Planning & iScenario

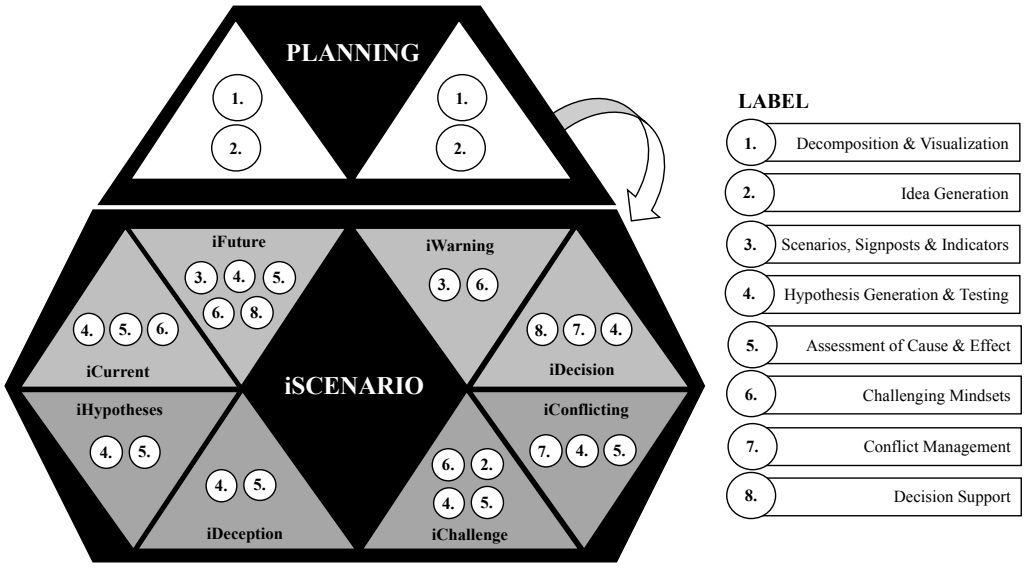

Figure 12 – iPentest: Planning & iScenario SAT

3.1.2. Threat Modeling phase

The Threat modeling phase defines a Threat Modeling approach for a correct execution of a Pentest as required on PTES. This phase offers a specific model, named iModeling Universe attributes, based on Intelligence techniques and built through the combination of recognized cyber security incident profiling taxonomies. Therefore, the iModeling Universe of attributes is a consistent model on the representation of its agents, capabilities and motivations; cyber threats, vulnerabilities, accesses and exploitability; operating and knowledge assets, informational, operational, business impact and risk rating scale.

The following section describes iModeling Universe of attributes classes, dimensions and attributes, while the subsequent section describes iModeling Universe of attributes Engine for which we used Intelligence techniques.

3.2. iModeling Universe of attributes

In this section it's explained how iModeling Universe of attributes was created (*see Figure 14 – iPentest: iModeling Universe of attributes*). Resulting from the multiple combination of recognized cyber security incident profiling taxonomies (**Howard & Longstaff, 1998; Lough, 2001; Stanton, et al., 2005; Harrison & White 2011; Mitre 2016; Enisa, 2018**), iModeling is predominantly represented by the following three classes: 1. Agent Profiling, 2. Attack Profiling, 3. Impact Profiling. Each one of these three classes have subclasses, where each subclass has dimensions and finally each dimension has several attributes (*see Figure 13 – iModeling Universe of attributes nomenclature*). Combining the attributes contained in each class, the result of iModeling offers a detailed cyber incident profiling that can be applied to different customer needs (Penetration testing mapping; Cybercriminal investigation; Cyber risk analysis).

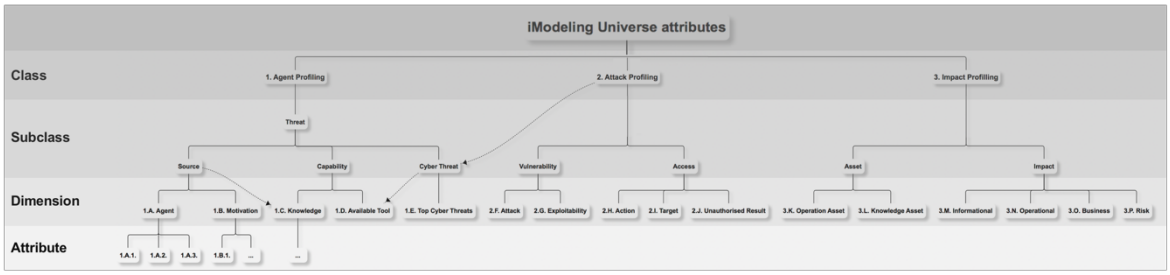

Figure 13 – iModeling Universe of attributes nomenclature

1. Agent Profiling

This profiling class offers a detailed characterization of human and cyber threats. It describes the Source of the attack, bearing in mind that we are only facing a threat if there is a human *Agent*, with *Motivation* and Capability to perform out the desired action. The Capability which is understood as the ability to successfully compromise the organization, depends on *agent's Knowledge* and *Available Tools* which are based on the existing Cyber Threats. The combination of these three subclasses (Source, Capability, Cyber Threat) provides organizations a clear illustration of the threats they face. These subclasses are divided into five dimensions: *Agent* (*Source*), *Motivation* (*Source*), *Knowledge* (Capability), *Available Tool* (Capability), Top Cyber Threats (Cyber Threat) (**Howard & Longstaff, 1998; Enisa, 2018**).

1.A. Agent (Source)

The *Agen*t dimension is related to the human threat, an individual or community of individuals (see *annex IV – Threat Modeling: Threat Agents/Community Analysis*; see *Table 2 – Agent Classification*). This dimension has the following attributes **(Howard & Longstaff, 1998; Nickerson et al., n.d)**:

1.A.1. External – includes script kiddies, hacktivists, Cybercriminals, nation states, cyber terrorists;

1.A.2. Internal – includes employees, management system administrators, developers, engineers, technicians;

1.A.3. Partners – includes competitors, suppliers, business vendors, outsourcing support.

AGENT CLASSIFICATION				
Threat Agents	**Examples**	**Characteristics**		
		Trust	**Privileges**	**Detailed Description**
External	− Script Kiddies − Hacktivists − Cybercriminals − Nation States − Cyber Terrorists	No	No	External individuals with malicious intends that collect publicly information to gain information about the corporation. This may include former employees with still-active access.
Internal	− Employees − Management − System Administrators − Developers − Engineers − Technicians	High	High	Persons working directly and inside the company with direct access to information about technology in use. Given their position and function inside the company they may have access to privileged information.

Partners	− Competitors − Suppliers and Vendors − Outsourcing Support	Mediu m	Medium	Business Partners may have access to corporate culture, information about technologies in use and other potential items of interested to successful execute the attack.

Table 2 – Agent Classification[9]

1.B. Motivation (Source)

The *Motivation* behind a cyber-attack is constantly changing and indicates whether the agent's intentions are deliberate or accidental. This dimension has the following attributes (**Gandhi et al, 2011; Nickerson, et al., n.d**):

1.B.1. Social-Cultural – includes attacks with philosophical, theological, and humanitarian goals, or are performed for fun, curiosity, desire for publicity or ego;

1.B.2. Economic **–** includes direct or indirect profit such as theft of intellectual property, economically valuable assets, fraud, espionage, sabotage, blackmailing, or economic recession and greed;

1.B.3. Political **–** include destroying, disrupting or taking control of targets, protests or retaliatory actions, cyberespionage and political statements;

1.B.4. Unaware **–** include insiders with unintentional actions or uninformed of security issues.

1.C. Knowledge (Capability)

This dimension defines the agent's level of cyber and kinetic knowledge to perform actions against the organization with proficiency. The *Knowledge* is quantified in the following three attributes (**Sandia, 2007**):

1.C.1. Low (L) **–** agent is capable of using novice proficiency to perform his actions. Agent has low to moderate of practical knowledge training and no theoretical knowledge;

1.C.2. Medium (M) – agent is capable of using intermediate proficiency to perform his actions. Agent has highly practical knowledge training and low to moderate theoretical knowledge;

1.C.3. High (H) **–** agent is capable of using expert proficiency to perform his actions. Agent has both expert practical and theoretical knowledge.

[9] Note: adapted from **Howard & Longstaff, 1998; Nickerson et al., n.d.**

1.D. Available Tools (Capability)

This dimension defines the mean used to exploit a computer or network vulnerability. Tools can also be more or less sophisticated, efficient and effective. This dimension has the following attributes (**Howard & Longstaff, 1998):**

1.D.1. Physical Attack;

1.D.2. Information Exchange;

1.D.3. User Command;

1.D.4. Script or Program;

1.D.5. Autonomous Agent;

1.D.6. Toolkit;

1.D.7. Distributed Tool;

1.D.8. Data Trap.

1.E. Top Cyber Threats (Cyber Threat)

This dimension represents the current threat landscape, resulting from the OSINT collection, analysis and assessment effort that has taken in place in the entire year of 2017. This dimension has the following attributes (**ENISA, 2018**):

1.E.1. Social Engineering (*see Annex IX– Social Engineering Attacks*);

1.E.2. Spam;

1.E.3. Identity Theft;

1.E.4. Information Leakage;

1.E.5. Data Breaches;

1.E.6. Web-based attacks;

1.E.7. Web-application attacks;

1.E.8. Malware;

1.E.9. Exploit Kits;

1.E.10. Denial of Service;

1.E.11. Botnets;

1.E.12. Ransomware;

1.E.13. Cyber Espionage.

2. Attack Profiling

This profiling class offers a detailed characterization of the attack, which mostly results from an unauthorized approach. It describes the existing *Vulnerabilities* and the actions to breach and gain *Access* to organization systems. The joint of these two subclasses (Vulnerability and Access) provides organizations a clear illustration of the attack vector. These subclasses are divided into five dimensions: *Attack* (*Vulnerability*), *Exploitability* (*Vulnerability*), *Action* (*Access*), *Target* (*Access*) and *Unauthorized Result* (*Access)* (**Howard & Longstaff, 1998**).

2.F. Vulnerability

This dimension represents system weaknesses that may result in unauthorized access to organization systems. This dimension has the following attributes (**CVE Details, 2017**):

2.F.1. Denial of Service*;*

2.F.2. Code Execution;

2.F.3. Buffer Overflow;

2.F.4. Memory Corruption;

2.F.5. SQL Injection;

2.F.6. Cross-Site Scripting (XSS);

2.F.7. Directory Transversal;

2.F.8. HTTP Response Splitting;

2.F.9. Bypass something;

2.F.10. Gain Information;

2.F.11. Gain Privileges;

2.F.12. File Inclusion;

2.F.13. Cross-Site Request Forgery (CSRF).

2.G. Exploitability

This dimension defines a temporal metric that is used to measure the likelihood of attacks against vulnerabilities based on the current state of exploitation techniques or code availability. This dimension has the following attributes (**FIRST, 2017**):

2.G.1. Not defined – does not influence*;*

2.G.2. Unproven – no exploitation code or theoretical code;

2.G.3. Proof-of-Concept – code is available but not functional in all situations, it requires substantial modification by a proficient threatening agent;

2.G.4. Functional – code is available and it works in most situations where the vulnerability exists;

2.G.5. High – autonomous functional code is available with no need for manual trigger, and works in every situation.

2.H. Action

This dimension represents agent's activities or processes that results in a change of systems status. This dimension has the following attributes (**Howard & Longstaff, 1998; IEEE, 2000**):

2.H.1. Probe – determine the characteristics of target*;*

2.H.2. Scan – determine which targets have a particular characteristic;

2.H.3. Flood – overload target's capacity;

2.H.4. Authenticate – accessing and assuming an authentication process;

2.H.5. Bypass – avoid a process using an alternative exploitation method to access a target;

2.H.6. Spoff – providing masquerade information to access the target;

2.H.7. Read – obtain content from the target;

2.H.8. Copy – reproduce content without changing the target;

2.H.9. Modify – change the content of a target;

2.H.10. Steal – take content from the target;

2.H.11. Delete – remove content from the target and make it irreversible.

2.I. Target

This dimension represents logical (L) or physical (P) entities for which the *Action* is directed. This dimension has the following attributes **(Howard & Longstaff, 1998):**

2.I.1. Account (L);

2.I.2. Process (L);

2.I.3. Data (L);

2.I.4. Component (P);

2.I.5. Computer (P);

2.I.6. Network (P);

2.I.7. Internetwork (P).

2.J. Unauthorized Result

This dimension represents the reasonable end of a successful attack. To achieve it, the *Agent* had to use an *Available Tool* to exploit a *Vulnerability* resulting in an unauthorized *Access* against a specific *Target.* This dimension has the following attributes **(Howard & Longstaff, 1998):**

2.J.1. Increased Access;

2.J.2. Disclosure of Information;

2.J.3. Corruption of Information;

2.J.4. Denial of Service;

2.J.5. Theft of Resources.

3. Impact Profiling

This profiling class offers a detailed characterization of impact. It describes *Assets* and the *Impact* if affected. *Assets* are the desired tangible or intangible (*operating and knowledge*) resources that may lead to several consequences if any kind of action against them occur. They are valuable to execute ongoing operations of a corporation, and consequently generate different kinds of *Impact* (*informational, operational and business*) to organizations. The joint of these two subclasses (Assets and Impact) provides organizations a clear illustration of cyber risk. These subclasses are divided into seven dimensions: *Operating Assets* (*Assets*),

Knowledge Assets (*Assets*), *Informational* (*Impact*), *Operational* (*Impact*), *Business* (*Impact*) and *Risk* (*Impact*) **(Nickerson, et al., n.d)**.

3.K. Operating Asset

This dimension represents tangible ongoing operation business assets. This dimension has the following attributes (**Baybutt, 2003; Nickerson, et al., n.d):**

3.K.1. Peopleware – such as Executive Management; Executive; Assistants; Middle Management; Administrative Assistants; Technical/Team Leads; Engineers; Technicians; Human Resources;

3.K.2. Client Software – such as Corporation Applications; Browser; Webmail; Cloud Services; Self-Service Kiosk;

3.K.3. Server Software – such as Server Information; Server Data Base;

3.K.4. Workstations – such as PCs, Laptops, Mobile, Tablets;

3.K.5. Servers – such as SCADA systems; Backups; Printers; Surveillance System;

3.K.6. Data Network Infrastructure – such as Wire system; Active Network Equipment, such as Hubs, Switch, Router, Bridge, Network Cards;

3.K.7. General support systems – such as HVAC; Humidity control, Smoke and fire detector; Halon system; Biometric Access; Electric Power; Backup Power Generation.

3.L. Knowledge Asset

This dimension represents intangible ongoing operation business assets. This dimension has the following attributes (**Nickerson, et al., n.d):**

3.L.1. Policies, Plans & Procedures;

3.K.2. Product Information;

3.K.3. Marketing Information;

3.K.4. Financial Information;

3.K.5. Technical Information;

3.K.6. Employee Data;

3.K.7. Customer Data.

3.M. Informational Impact

This dimension consists in the characterization of information security elements (CIA triad). This dimension has the following attributes (**ISO/IEC 27001:2013**):

3.M.1. Confidentiality – assure data is confidential and held by individuals that are authorized. For instance, disclosure of information affects Confidentiality;

3.M.2. Integrity – assure that people are not intentionally or accidentally tampering with the data that the organization holds. For instance, log tampering, modify data, configurations or privileges, fraudulent transactions, software installation and misappropriation affects Integrity;

3.M.3. Availability – assure data is not lost with redundancy of systems and backups. For instance, destruction, loss, interruption, degradation and encryption affects Availability.

3.N. Operational Impact

This dimension consists in the characterization of the operational impact to the organization. This dimension has the following attributes (**Simmons et al, 2009**):

3.N.1. Misuse of Resources – abusive and unauthorized actions related to certain functions and privileges;

3.N.2. User Compromise – unauthorized access and use of a specific host privilege;

3.N.3. Root Compromise – unauthorized action against a System that to gain Administrative Privileges;

3.N.4. Web Compromise – website or Web application vulnerabilities exploitation to compromise Information;

3.N.5. Installed Malware – gain full control of the compromised system to access to Sensitive information or remote control of the host (e.g. Virus; Spyware; Trojan; Worms; Arbitrary Code);

3.N.6. Denial of Service – deny access to a particular resource or service (e.g. Host based; Network Based; DDoS).

3.O. Business Impact

This dimension consists in the characterization of potential consequences for the business model. This dimension has the following attributes (**Nickerson, et al., n.d**):

3.O.1. Nuisance;

3.O.2. Damage to Reputation and Confidence;

3.O.3. Compliance or Regulatory Incidents;

3.O.4. Loss of Intellectual Property;

3.O.5. Production Disruption;

3.O.6. Physical Equipment Damage;

3.O.7. Financial Losses;

3.O.8. Data Destruction and Loss of Data Integrity;

3.O.9. System Sabotage or Shutdown.

3.P. Risk

This dimension defines a metric that is used to assess the risk of controls being compromised and its financial consequences. This dimension has the following attributes **(ISO 15408:2005; Nickerson, et al., n.d):**

3.P.1. Low – Low risk of security being compromised; Negative Impact as result;

3.P.2. Moderate – Moderate risk of security being compromised; Limited financial losses as result;

3.P.3. Elevated – Elevated risk of security being compromised; Material financial losses as result;

3.P.4. High – High risk of security being compromised; Significant financial losses as result;

3.P.5. Extreme – Extreme risk of security being compromised; Catastrophic financial losses as result.

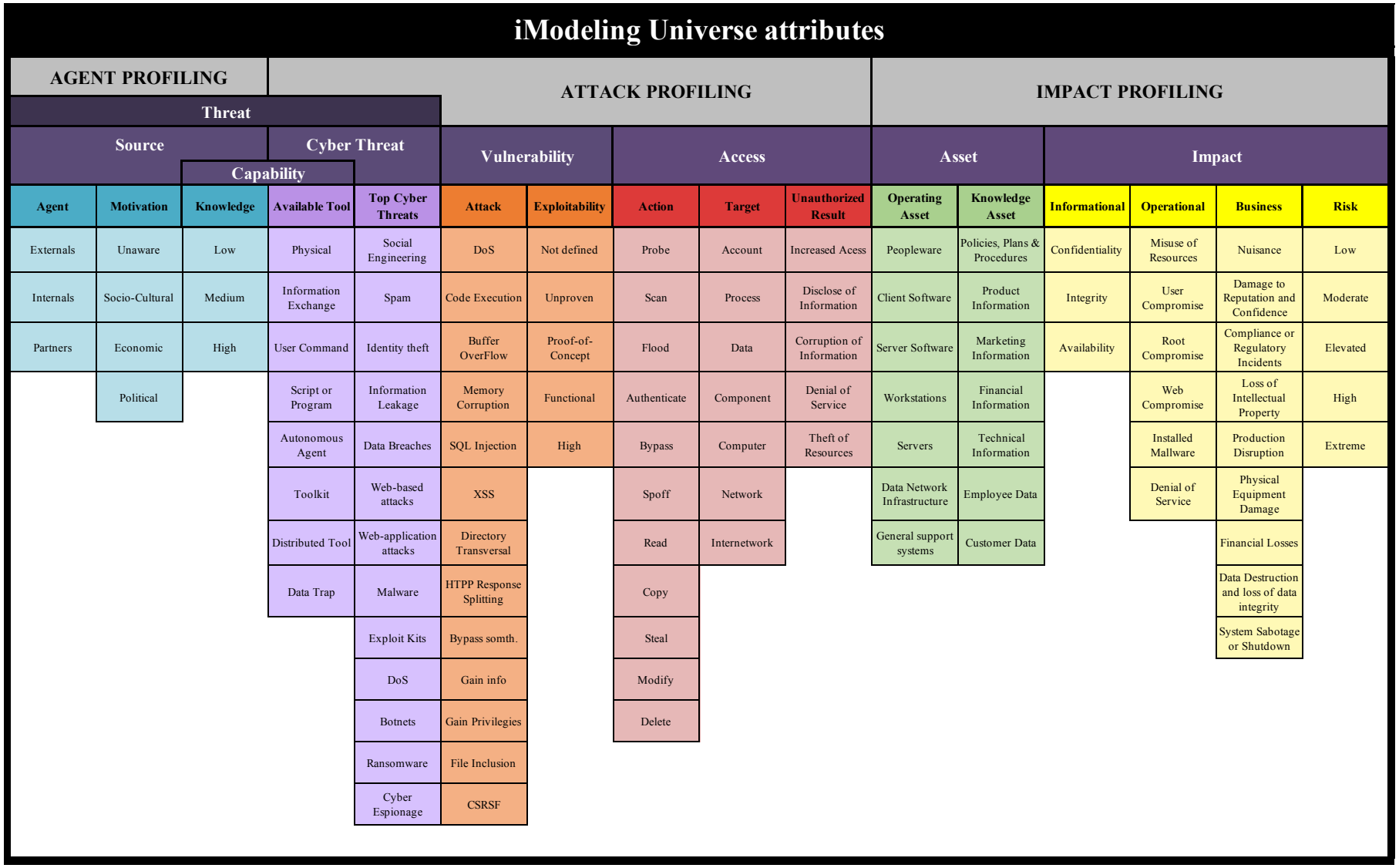

Figure 14 – iPentest: iModeling Universe of attributes

3.2.1. iModeling Universe of attributes Engine

This section offers a conceptual review and analysis about iModeling Universe of attributes Engine for which we used SAT. In the previous chapter we presented eight categories of SAT (see section *2.2.5. Structured Analytic Techniques*), each one containing several different techniques. However, there is a specific technique that is used for modeling complex social and organizational planning problems that are not easily quantifiable (often called "wicked problems" or "social messes"). Wicked problems are about issues that cannot be quantified, containing complex uncertainties and dependent of its stakeholders. For instance, threat assessment, social perceptions or technological development.

Turns that, the General Morphological Analysis (GMA; developed by Fritz Zwicky[10]) brings us the solution to deal with such problems. This method has been applied by Zwicky on several fields, such as classification of astrophysical objects[11] and development of new forms of propulsive power systems[12]. Later, GMA started to be used by several engineers, operational researchers, and by a large number of researchers in the field of policy analysis and future projections. Most recently, with the advances on computer support the creation of non-quantified inference models became promising, extending GMA functionalities and its range of application (**Rhyne, 1981; Coyle, 1996; Ritchey, 2011)**.

This method, GMA, analyzes and model complex social, organizational and political systems by decomposing the problem into a problem space, and then examines the total set of possible relationships between attributes in that problem space. The process for creating the problem space goes through a cycle of two principles: (i) analysis; and (ii) analysis-synthesis (**Zwicky, 1966; Heuer & Pherson, 2014**).

(i). GMA Analysis phase (decomposition)

The analysis principle consists on identifying and defining the most important dimensions. Then each dimension should be decomposed into a spectrum of attributes that will represent the parameter space of the problem in need of investigation. Then, this information should be organized in the morphological field (also named Zwicky box) into a *n*-dimensional morphological field (see *Table 3 – 4-dimension Morphological Field*).

[10] Zwicky, F. (1948). **The Morphological Method of Analysis and Construction**. Courant. Anniversary Volume. New York: Intersciences Publish. pp. 461-470.
[11] Zwicky, F. (1948). **Morphological Astronomy**. The Observatory. Vol. 68, No. 845. pp. 121-143
[12] Zwicky, F. (1948). **Morphology of aerial propulsion**. Helvetica Physica Acta. Vol. XXI, Heft 5. pp. 299-340.

Dimension A	Dimension B	Dimension C	Dimension D
Attribute A.1	Attribute B.1.	Attribute C.1.	Attribute D.1.
Attribute A.2	Attribute B.2.	Attribute C.2.	Attribute D.2.
Attribute A.3		Attribute C.3.	Attribute D.3.
			Attribute D.4.

Table 3 – 4-dimension Morphological Field[13]

The next step, is to calculate the total number of simple configurations (T_c) from our morphological field (N). Considering the number of parameters in the morphological field (N), and the number of attributes (A_x) in the value range of a dimension, the total number of simple configurations (T_c) in the morphological field is calculated by the following equation:

$$\mathbf{Tc} = \prod_{i=1}^{N} Ai$$

The result from the previous calculus demonstrates that the 4-dimension morphological field (N=4) from our example has $T_c = 72$ possible simple configurations[14]. The colored cells in this field shows one variable from each dimension and therefore one possible solution to the complex problem (**Richey, T. 2011**).

However, we already know that our complex problem relies on finding a solution to fill the gap found on the PTES Threat Modeling phase. The research for this problem resulted in the iModeling Universe (Figure 14 – iPentest: iModeling Universe attributes) for which we know that has 16-dimension morphological field (N=16). Applying the previous calculus, iModeling Universe has $\mathrm{Tc} = 3{,}7187e^{12}$ possible configurations[15].

The main problem is that as the number of dimensions increases, the number of simple configurations increases as well, which makes difficult to analyze all these configurations by hand.

[13] Note. The colored cells define one of all the possible combinations. Adapted from **Ritchey, 2011.**

[14] Calculated through: $T_c = 3 \times 2 \times 3 \times 4 = 72$

[15] Calculated through: $\mathrm{Tc} = 3 \times 4 \times 3 \times 8 \times 13 \times 13 \times 5 \times 11 \times 7 \times 3 \times 7 \times 7 \times 3 \times 6 \times 9 \times 5 = 3{,}7187e^{12}$

(ii). GMA analysis-synthesis principle

The analysis-synthesis principle consists in examining the relationships between these attributes, which will significantly reduce the field by identifying all mutually contradictory conditions. This principle will not be performed on this research but it's explained how theoretically works.

As mentioned, this principle requires that every attribute from the morphological field should be paired with another, excluding all non-possible relationships between attributes, which makes the total solution space smaller and more consistent.

This principle uses a process named Cross-Consistency Assessment (CCA) which is used to check the integrity, clarity the concepts and to identify incompatible relationships between attributes. The Cross-Consistency matrix (CCM) works as an accounting table for the CCA process (*see Figure 15 – Cross-Consistency Matrix for 4-dimension Morphological Field*). CCM can be seen as a relational database and used as a high-level relational knowledge base (gathering typologies about the relation between attributes from the complex problem under investigation).

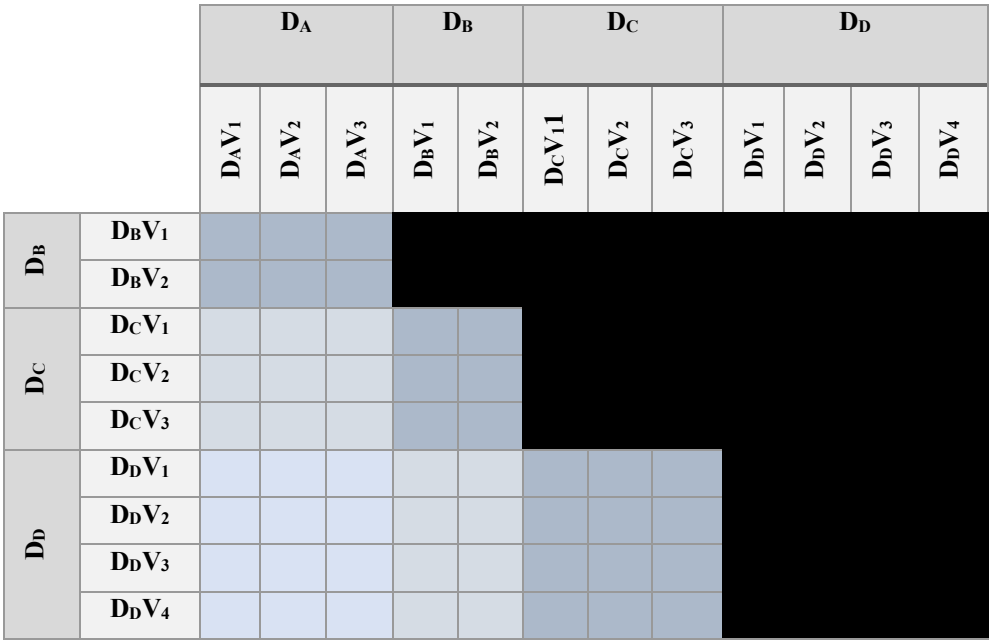

Figure 15 – Cross-Consistency Matrix for 4-dimension Morphological Field

The CCA process involves two assessment phases: (1) to determine the total number of parameters blocks that are connected and which are not; (2) to identify and flag incompatible pairs of values.

Phase 1 – Total nº. Parameters Block (PB)

The CCM cross-references the value range of each pair of parameters which is called parameter block (PB) and the number of PB in the CCM is calculated through the following expression (represents the total number of possible relationships between those dimensions):

$$\mathbf{PB} = \frac{\mathbf{1}}{\mathbf{2}}\boldsymbol{N}\ (\boldsymbol{N}-\mathbf{1})$$

Taking in account the "*Table 3 – 4-dimension Morphological Field"*, this morphological field (N=4) contains PB= $\frac{1}{2}4\ (4-1)=6$. Applying the same calculus to iModeling Universe, the morphologic field (N=16) contains PB= $\frac{1}{2}16\ (16-1)=120$.

Phase 2 – Total nº. Dyadic Relationships (Dt)

It is necessary to identify the total number of invalid configurations. The total number of dyadic (pairwise) relationships (Dt) between all attributes in the cross-consistency matrix is calculated through the following expression:

$$\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} \boldsymbol{vi}\times\boldsymbol{vj}$$

The 4-dimension morphological field (N=4) contains 3,2,3,4 attributes, so D_t= 144. Applying the same calculus to iModeling Universe, the morphologic field (N=16) contains 3,4,3,8,13,13,5,11,7,5,7,7,3,6,9,5 attributes, so Dt= 5354.

In sum, morphological models have the following four formal properties (see *Table 4 – Four Formal Properties of iModeling CCA*):

iModeling Properties		
Parameters in the Morphological Field (N)	**N**	16
Parameter Block (PB)	$\frac{\mathbf{1}}{\mathbf{2}}\boldsymbol{N}\ (\boldsymbol{N}-\mathbf{1})$	120
Dyadic Relationships (Dt)	$\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} \boldsymbol{vi}\times\boldsymbol{vj}$	5354
Total nº of Simple Configurations (Tc)	**Tc = V1 × V2 …VN**	$3{,}7187e^{12}$

Table 4 – Four Formal Properties of iModeling CCA

Applying CCA technique to morphological fields makes possible to identify variables that have plausible, practicable and valid relationships, and to identify those which have no link at all. This connectivity can reduce by to 90% or even 99% the space solution, providing reliable conduits of information and consequently more accurate results (**Heuer & Pherson, 2014; Richey & Alvarez, 2015).**

4. iPENTEST EVALUATION

This chapter aims to evaluate the iPentest proposal, in particular our proposal for the Threat Modeling phase, the iModeling Universe attributes. This proposal, henceforth named iModeling is going to be evaluated through the creation and analysis of case studies as proof-of-concept.

The main objective of this chapter is to provide means to understand complex cyber security problems with greater clarity, elucidate about previously hidden issues, and to extrapolate key results to support foreseeing.

To encompasses diverse perspectives of cyber security incidents, this chapter is divided into three case studies concerning each iModeling applicability: (1) Penetration testing mapping; (2) Cybercriminal investigation; (3) Cyber risk analysis.

Each case study is divided into three sections, described as follows:

(i). Description – in this section, the case study background and major findings (evidences) are briefly clarified. Also, the subject of analysis or object under investigation is described.

(ii). Modeling – in this section, iModeling is used to outline possible scenarios using the existing evidences. The total number of scenarios and other formal properties of iModeling are also calculated. The links between the attribute were not assessed through the cross-consistency assessment. Instead, cyber security professionals provided them expertise to reduce the total solution space. These links were assessed considering four level of credibility: evidences, high and moderate and low confidence traces (see *Figure 31 – Hypotheses Credibility*; see *Table 5 – Assumptions quantification)*.

(iii). Analysis – in this section, iModeling Universe of attributes scenarios are explained and discussed.

Hypotheses Credibility Quantification	
Evidence	100% certainty
High confidence traces	Between 90% to 100%
Moderate confidence traces	Between 50% to 90%
Low confidence traces	Less than 50%

Table 5 – Assumptions quantification

4.1. Case Study 1 – Penetration testing mapping

There are several advantages related to security audits, such as Penetration tests. The objective is to reveal weaknesses in computer science systems that could lead to data breach and other malicious intrusions. Once these vulnerabilities have been identified, the Pentester tries to exploit them to assess the technological capabilities that hackers need to proficiently compromise those systems, showing this way the real security business risk. Thereby, it makes possible to implement recommendations, controls and policies to improve the overall security, which is particularly important to ensure the continuity of business that has an online presence.

4.1.1. Description

Over the past decade, eCommerce brought essential changes to the way businesses are conducted. The continuous advances of technology and Internet results in many benefits for eCommerce sales. For instance, this new reality makes possible to create a startup at a low financial cost compared to all the costs related to physical shops. Moreover, online stores bring the opportunity to offer personalized customer experience, increasing revenues and customer loyalty. But when a business engages in eCommerce it faces many new risks, thus addressing those risks with appropriate security and control measures should be the businesses priority. The most common cybernetic risks of running an online shop are related to online security, system reliability, credit card fraud, privacy issues among other risks related to the business operationality. As proof-of-concept, the iModeling was applied to a Portuguese online shop website related to the sale of Gems, Crystals and handmade jewelry. In order to reach more consumers, this company, henceforth named G&C, recently changed its business model by expanding the business to an online store. Worried about the security issues G&C's CEOs have asked for a security audit of their website. The iModeling was applied on G&C website to test its current security status.

4.1.2. Modeling

The modeling process takes as starting point the iModeling solution space, where we introduce the evidences we collected during this investigation (see *Figure 16 – iModeling application: G&C's website pentest*).

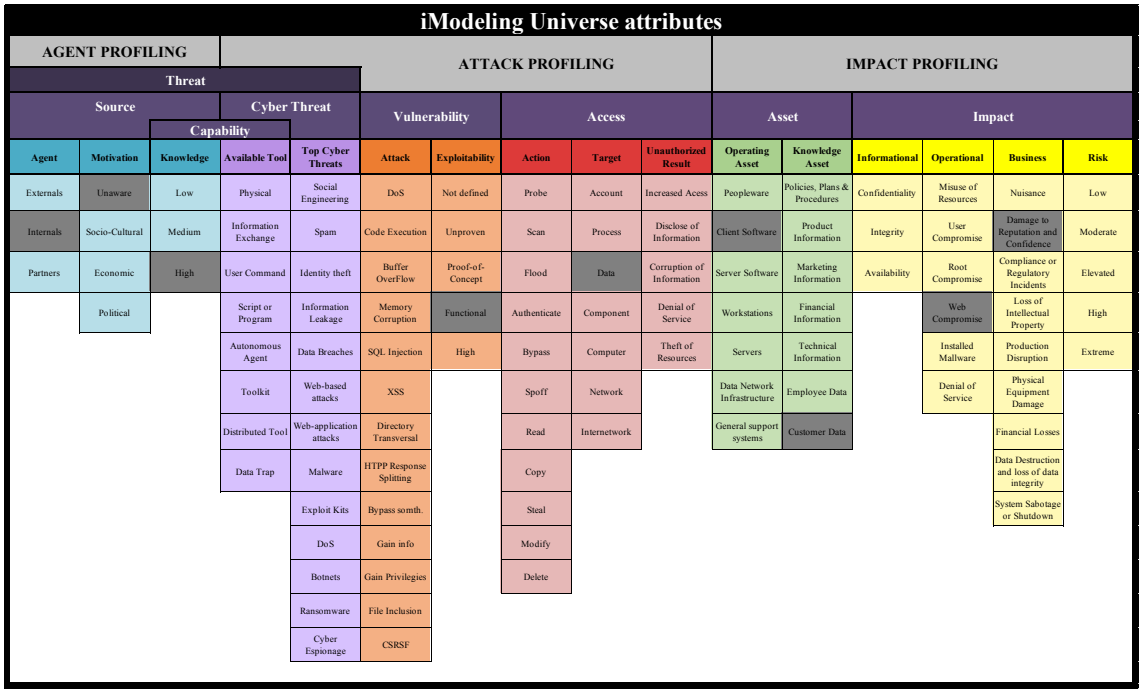

Figure 16 – iModeling application: G&C's website pentest

Applying iModeling on G&C's website we have nine known evidences. The remaining dimensions from iModeling field (N=7) will be considered to generate all the possible scenarios (Tc = 1115400) (see *Table 6 – iModeling CCA: G&C's website pentest*).

Parameters in the Morphological Field (N)	7
Parameter Block (PB)	21
Dyadic Relationships Dt)	2828
Total nº of Simple Configurations (Tc)	1115400

Table 6 – iModeling CCA: G&C's website pentest

The total number of possible scenarios is still too high to be processed by hand. Therefore, the next step in this process would be the creation of cross consistency matrix which would examine all the internal relationships between the remaining seven dimensions considering three levels of confidence (high, moderate and low confidence). This process would largely reduce the possible total number of simple configurations and automate of iModeling output scenarios. So, when the Pentester introduces the seven known evidences, the iModeling automatically gives output scenarios with three levels of confidence. However, the analysis

of the internal relations between attributes found on the remaining dimensions were not included on this case study. The following illustration represents three possible scenarios for G&C's penetration mapping (see *Figure 17 – iModeling scenarios: G&C's website pentest*).

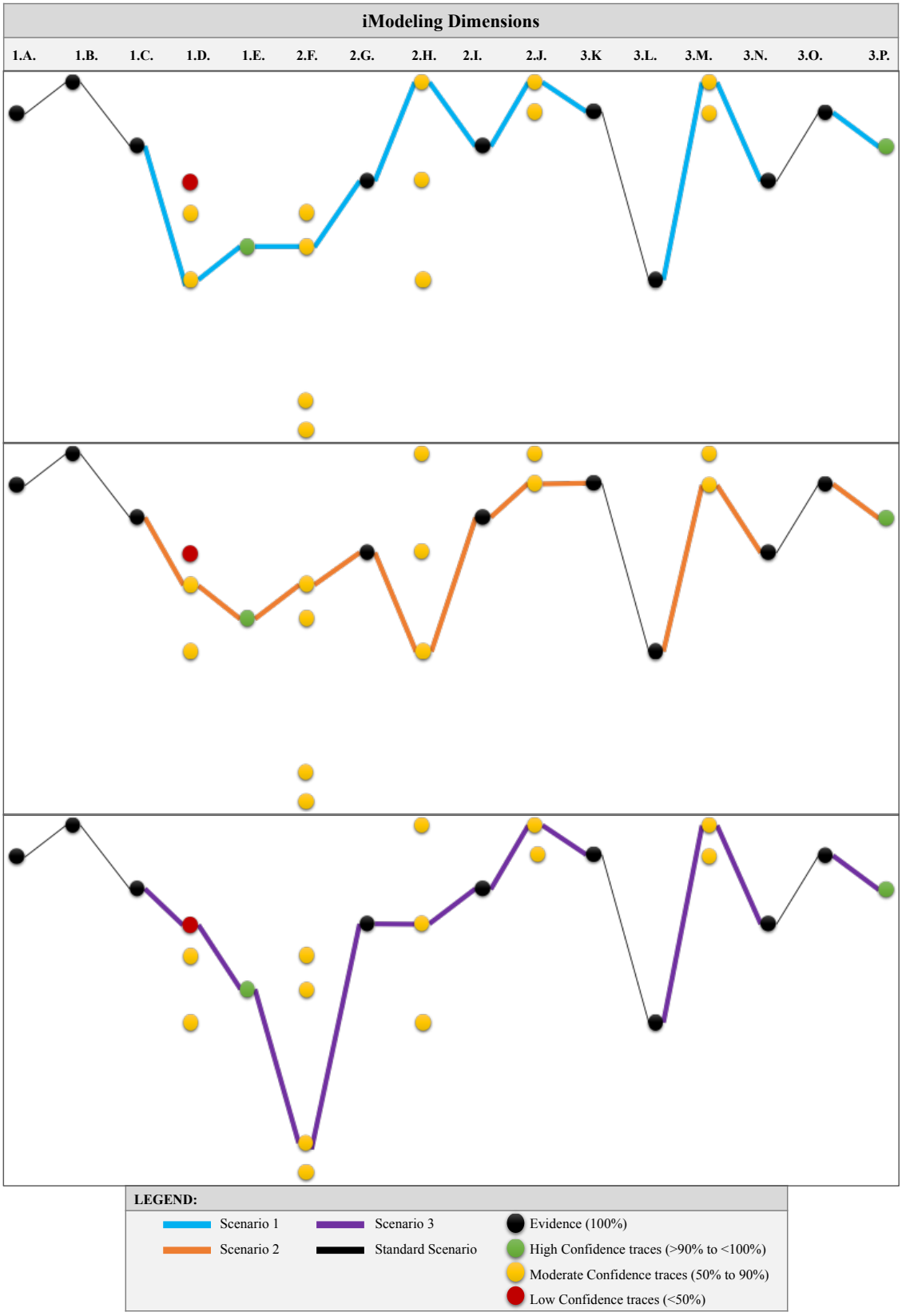

Figure 17 – iModeling scenarios: G&C's website pentest

4.1.3. Analysis

The analysis was carried out considering three different scenarios to support the explanation of G&C's website penetration test results.

Analysis of scenario 1

(1) Agent profiling: in this scenario the source of attack is an authorized Pentester, with a high level of practical and theoretical knowledge to perform the security audit to G&C's website.

(2) Attack profiling: this scenario shows that G&C's website is vulnerable to cross-site scripting (XSS). During the exploitation phase, the Pentester verifies that it could be possible to use tools to get zombie browsers via XSS (distributed tool). XSS is a type of computer security vulnerability that enables attackers to inject client-side scripts into web pages. The Pentester verifies there is no user's input validation (filtration). Consequently, it will be possible to inject scripts to steal user information (cookies, root credentials, etc).

(3) Impact profiling: if an external source successfully exploits the described vulnerability it might affect customer's data confidentiality. There is an elevated risk of compromising security through this method.

Analysis of scenario 2

(1) Agent profiling: as described in scenario 1.

(2) Attack profiling: this scenario shows that G&C's website is vulnerable to SQL injection. During the exploitation phase, the Pentester verifies that it could be possible to use autonomous SQL injection tools that both detects and exploits SQL injection flaws. This method is often used to extract data when the host website accepts user inputs, as verified with G&C's website.

(3) Impact profiling: if an external source successful exploit the described vulnerability it might affect customer's data integrity. There is an elevated risk of compromising security through this method.

Analysis of scenario 3

(1) Agent profiling: as described in scenario 1.

(2) Attack profiling: this scenario shows that G&C's website is vulnerable to brute force attacks. During the exploitation phase, the Pentester verifies that it could be possible to set

up customized scripts that successively try different username and password combinations until a match is discovered (gain privileges) and resulting in an unauthorized access to G&C's website (unauthorized authentication).

(3) Impact profiling: as described in scenario 2.

4.2. Case Study 2 – Cybercriminal investigation

We are living in a modern era based on technology where cybercriminals use Internet and computer technology to gain illicit advantages. We are facing a parallel form of living that grows up at a rampant volume and pace. Cybercrime is emerging as a serious threat in the society. It's the revolution of conventional crimes where computer is used as tool, as the target of crime, or both. Cybercriminals can commit malicious acts with near impunity, mostly because there are several barriers on cybercrime investigation. This is one of the hardest tasks for law enforcement agencies, starting on the legal system that has been forged in the physical world for physical crimes over centuries, while the Internet has less than three decades old.

Cybercriminals are often seen as faceless computer geeks hiding behind a computer, but there are individuals involved in cybercrime that aren't necessarily sophisticated. Contextualizing threats, motivations and capability to perform malicious acts is the key to crack cybercrime.

iModeling Universe of attributes proposal offers to cybercrime investigators the ability to contextualize cybercriminals and their threats based upon existing evidences. Modeling real-world cybercrimes allows a satisfactory explanation of a case which may involve many other crimes and investigations.

4.2.1. Description

As proof-of-concept, the iModeling was applied on an Electrical Household Appliances Company, henceforth named as EHAC18. This company has recently received a massive email spam attack which led to the unavailability of email service. EHAC18 couldn't use the email service for two business days. The email is a critical asset for this company as they receive several service markings for the domiciles of their customers and requests for business units. It is known that the email service and EHAC18 website is from an outsourcing server hosting. This company leads this business market and there aren't known competitors with malicious intentions. The iModeling have been used to find plausible interpretations that explain how this security incident happened, aiding the criminal investigation on course.

4.2.2. Modeling

The modeling process takes as starting point the iModeling solution space, where we introduce the evidences we collected during this investigation (see *Figure 18 – iModeling application: EHAC18*).

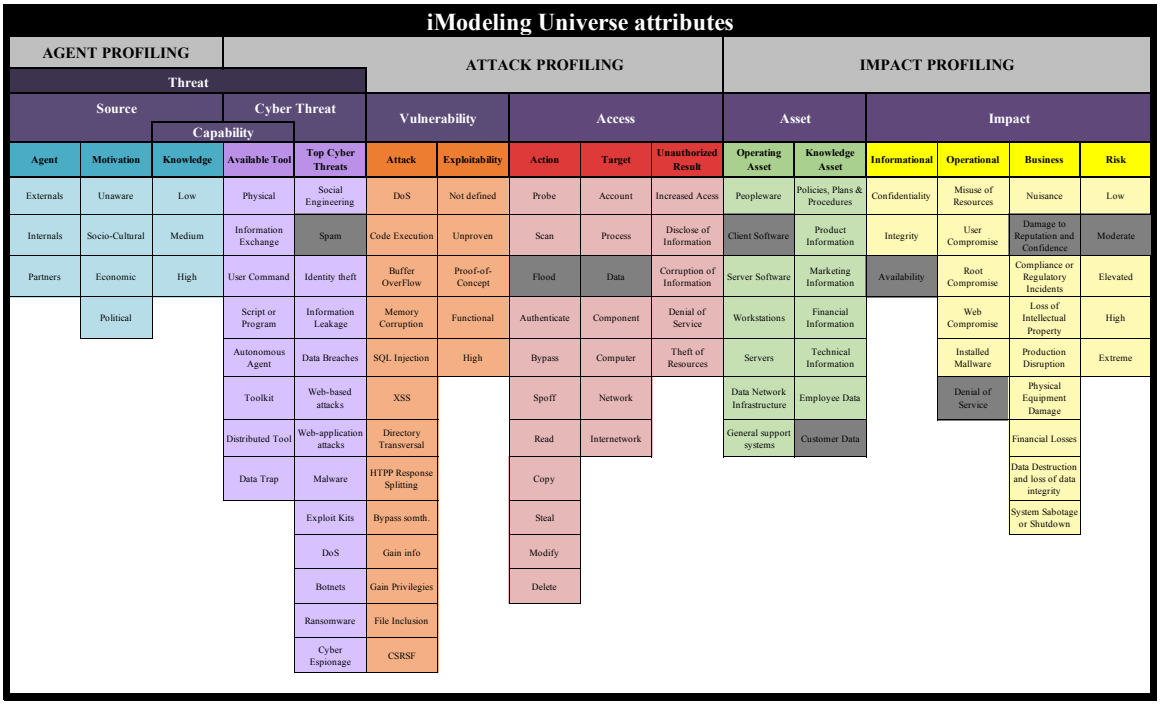

Figure 18 – iModeling application: EHAC18

Applying iModeling on EHAC18's cybercriminal investigation we have nine known evidences. The remaining dimensions from iModeling field (N=7) will be considered to generate all the possible scenarios (Tc = 93600) (see *Table 7 – iModeling CCA: EHAC18*).

Parameters in the Morphological Field (N)	7
Parameter Block (PB)	21
Dyadic Relationships Dt)	3009
Total nº of Simple Configurations (Tc)	93600

Table 7 – iModeling CCA: EHAC18

The total number of possible scenarios is still too high to be processed by hand. Consequently, the next step in this process would be the creation of cross consistency matrix which would examine all the internal relationships between the remaining seven dimensions considering three levels of confidence (high, moderate and low confidence). This process would largely reduce the possible total number of simple configurations and automate of iModeling output scenarios. So, when the investigator responsible for this criminal process introduces the seven known evidences, the iModeling gives output scenarios with three

levels of confidence. However, the analysis of the internal relations between attributes found on the remaining dimensions were not part of this case study. The following illustration represents three possible scenarios for EHAC18's cybercriminal investigation (see *Figure 19 – iModeling scenarios: EHAC18*).

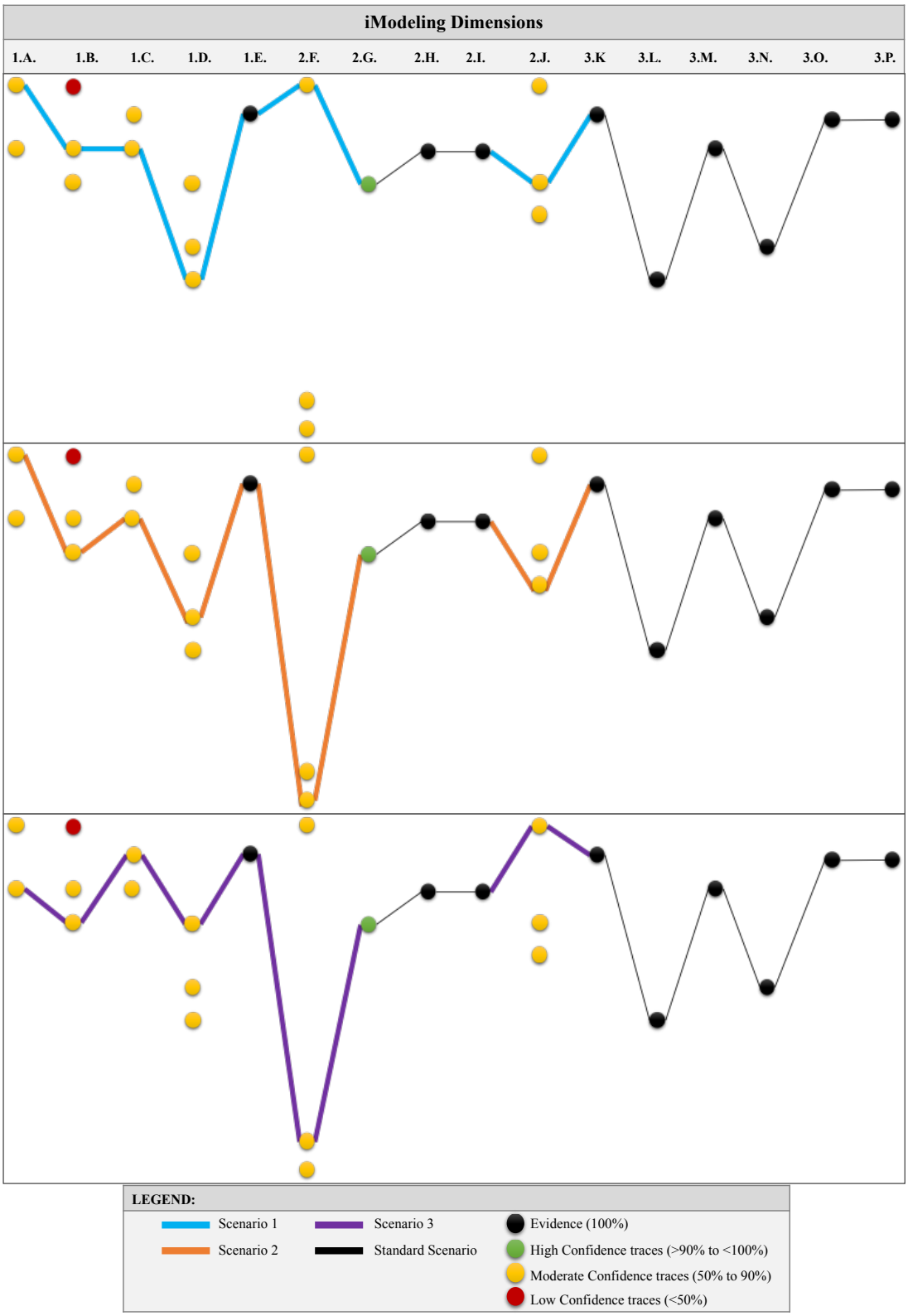

Figure 19 – iModeling scenarios: EHAC18

4.2.3. Analysis

The analysis is carried out considering three different scenarios to find plausible explanations for EHAC18's security incident and their implications.

Analysis of scenario 1

(1) Agent profiling: the source of the threat is described as an external malicious agent with the main motivation of making profit (economic motivations) and has a high level of practical and theoretical knowledge.

(2) Attack profiling: the tool used to the execution of this attack is described as a spambot (distributed tool) which automatically gathers extensive lists of random email addresses and then uses legitimate SMTP (Simple Mail Transfer Protocol) credentials to masquerade spam messages as legitimate emails. This spam attack is functional and successfully floods the mailbox and overwhelm the server on which the EHAC18's mailbox is hosted (theft of resources).

(3) Impact profiling: through the existing evidences the impact resulting from this security incident is described. EAHC18' employees couldn't access to email requests from its customers and partners (data availability) during two business days. This led to limited costs in the remediation of this as well as lost reputation and customer loyalty (moderate risk).

Analysis of scenario 2

(1) Agent profiling: the source of the threat is described as an external malicious agent with the main motivation of disrupting EAHC18' services (politic motivations) and has a high level of practical and theoretical knowledge.

(2) Attack profiling: the attacker used a malware toolkit to successfully infect the email server through a link or a file send for an email (file inclusion). This spam attack effectively theft email server resources.

(3) Impact profiling: as described in scenario 1.

Analysis of scenario 3

(1) Agent profiling: the source of the threat is described as a business partner agent with the main motivation of taking control of EAHC18' email service (political motivations). The agent has high level of practical but intermediate level of theoretical knowledge.

(2) Attack profiling: the attacker used a known email server vulnerability (customized program) to successfully gain privileges over EAHC18' email server which led the email server to be compromised (increased access) by being sent spam.

(3) Impact profiling: as described in scenario 1.

4.3. Case Study 3 – Cyber risk analysis

Cyber threats are one of the most highly and impactfully source of cyber risk. Understanding and managing the cyber risk is a fundamental shift for organizations. Businesses are investing in technology to gain a competitive advantage in their given markets but not to protect their information systems. Business managers should understand the root cause and magnitude of cyber risks and consider its impact on their organizations. Cyber risk is usually defined as exposure to harm or financial losses resulting from vulnerabilities and attacks to information systems.

There are many benefits of making cyber risk assessments beyond simply complying with government regulations. It has become clear that today's organizations can no longer wait when it comes to cyber security. A comprehensive review of administrative, technical, and physical security are now necessary safeguards and protocols to protect organizations, their employees, customers and business partners. However, a strategic shift is required to be prepared to deal with serious cyber issues and vulnerabilities and then make more informed decisions. For instance, strengthen security requirements any time personal or sensitive information needs to be exchanged or shared within the organization and their partners. Organizations should use these cyber security risk assessments to create their competitive advantage.

iModeling proposal offers organizations the ability to characterize business assets and process threats, and their impact on the organization. iModeling uses the existing evidences to evaluate the impact.

4.3.1. Description

As proof-of-concept, iModeling was applied to the Alcácer do Sal City Hall, the municipal council of this City Hall, henceforth named as AS City Hall.

The AS City Hall is responsible for protecting their information systems and the personal data of its employees and citizens they have to handle every day. Concerned about the cybersecurity risk, they invest in the adoption of information systems security policies, promoting regularly awareness of privacy and data protection issues among its employees and partners. We asked to the AS City Hal's IT department for their collaboration to apply iModeling. As they often perform penetration tests to identify potential vulnerabilities and continuously improve the security of their technological infrastructures we could apply our model as a risk analysis framework to any asset threats on their infrastructure. So, during a

penetration test they found a vulnerability on their website concerning brute force attack. This vulnerability was successful exploited using scripts that uses different word dictionaries until find the password to login on their systems. Through consecutive attempts, they were able to successful access the administrator password and once inside the systems with root access a potential external threat could do everything with the information available (citizens and employees' information, and data on local lodgings and restaurants).

4.3.2. Modeling

The modeling process takes as starting point the iModeling Universe attributes, where we introduce the evidences that were collected during the cyber risk assessment (see *Figure 20 – iModeling application: AS City Hall*).

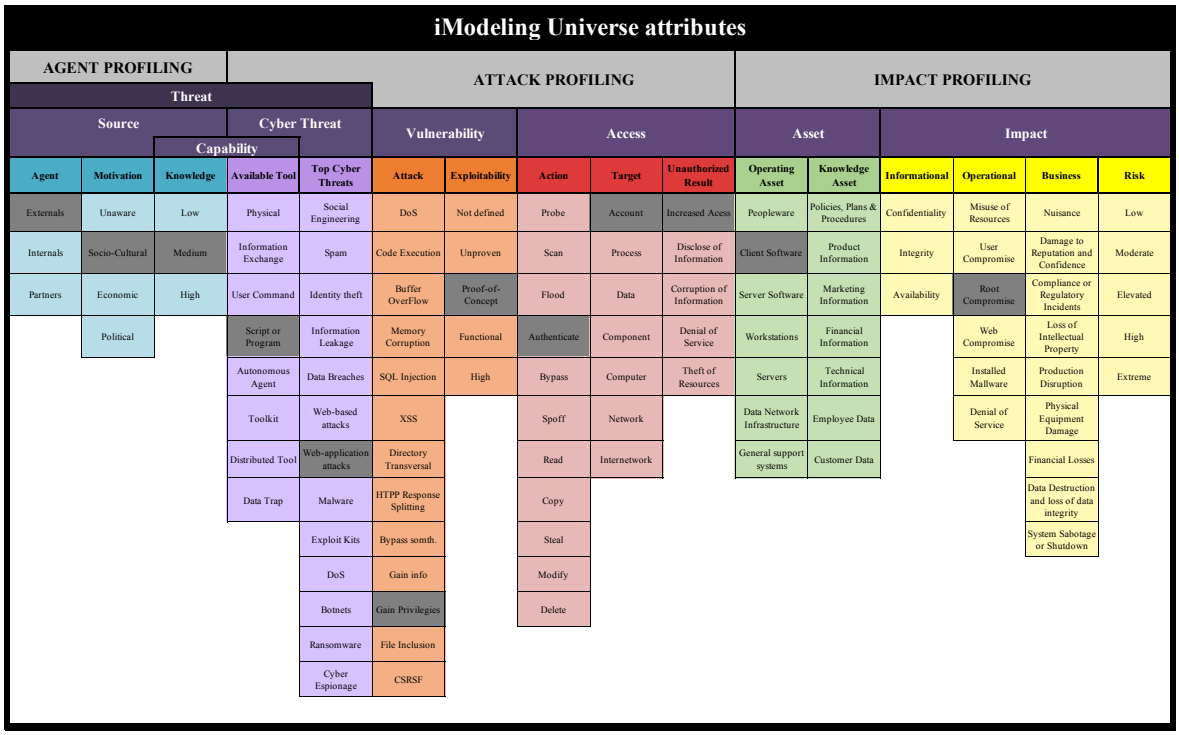

Figure 20 – iModeling application: AS City Hall

Applying iModeling on the AS City Hall's cyber risk assessment we have twelve known evidences. The remaining dimensions from iModeling field (N=4) will be considered to generate all the possible scenarios (Tc = 945) (see *Table 8 – iModeling CCA: AS City Hall*).

Parameters in the Morphological Field (N)	4
Parameter Block (PB)	6
Dyadic Relationships Dt)	266
Total nº of Simple Configurations (Tc)	945

Table 8 – iModeling CCA: AS City Hall

The total number of possible scenarios is still too high to be processed by hand. Consequently, the next step in this process would be the creation of cross consistency matrix which would examine all the internal relationships between the remaining four dimensions considering three levels of confidence (high, moderate and low confidence). This process would largely reduce the possible total number of simple configurations and automate of iModeling Universe of attributes output scenarios. So, when the cyber risk auditor or the Pentester introduces the twelve known evidences, the iModeling automatically gives output scenarios with three levels of confidence. However, the analysis of the internal relations between attributes found on the remaining dimensions were not part of this case study. The following illustration represents three possible scenarios for the AS City Hall cyber risk analysis (see *Figure 21 – iModeling scenarios: AS City Hall*).

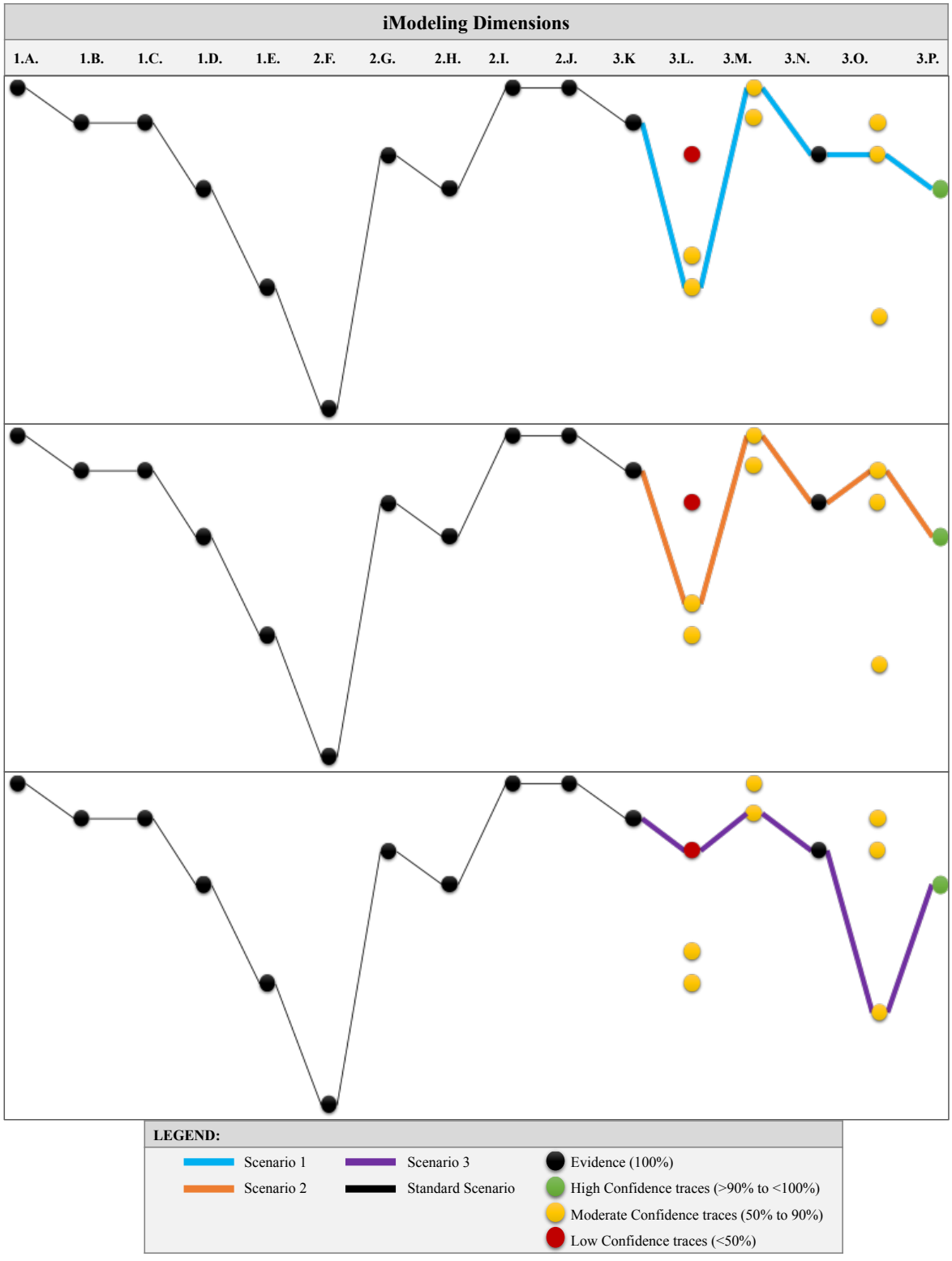

Figure 21 – iModeling scenarios: AS City Hall

4.3.3. Analysis

The analysis is carried out considering three different scenarios to find plausible explanations for the AS City Hall cyber risk assessment. For this case study, we have all details about the Agent and Attack profiling. Therefore, this analysis covers only the impact profiling.

Analysis of scenario 1

(1) Agent Profiling: the AS City Hall confirmed that the agent could be any external source with a high practical knowledge training and low to moderate theoretical knowledge and with desire to execute malicious actions for fun and curiosity.

(2) Attack Profiling: during its Pentesting, the AS City Hall confirmed that a vulnerability on their website concerning the brute force attack. Through this vulnerability they could use a script to gain a privileged access and authenticate into their systems.

(3) Impact profiling: the result of the technical security assessment of the AS City Hall reveal that a successful brute-force could affect the confidentiality of the data of its citizens. Even though passwords policy is not specifically mentioned on the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), it requires a high level of protection for personal data. It has been verified that the AS City Hall has a high risk of security compromising and at the same time, in compliance with the GDPR, it has a high risk of being fined, confirmed through the Pentest results.

Analysis of scenario 2

(1) and (2) as described in scenario 1.

(3) Impact profiling: the result of the technical security assessment of the AS City Hall reveal that a successful brute-force could affect the confidentiality of the sensitive data of its employees. As result it may lead to the loss of confidence of the employees. It has been verified that the AS City Hall has a high risk of security compromising by external agents.

Analysis of scenario 3

(1) and (2) as described in scenario 1.

(3) Impact profiling: the result of the technical security assessment of the AS City Hall reveal that a successful brute-force could affect the integrity of data and information regarding accommodation and restaurants in the municipality of Alcácer do Sal. These data

could be destroyed or altered thereby producing false information. It has been verified that the AS City Hall has a high risk of security compromising by external agents.

5. CONCLUSIONS

While reviewing the PTES recommendation we found relevant to create a proposal model for the PTES Threat Modeling phase. Moreover, we realized that it could be possible to merge different fields of expertise such as Penetration tests and Intelligence. To our knowledge, we merged for the first time such different fields, which is an important finding by adding new knowledge to the field and increases the motivation to look for the correlation between different knowledge domains and create common features of application.

After examining the existing Intelligence techniques, we showed that is possible to apply those techniques (SAT) to the construction of a threat modeling approach, maintaining its consistency in terms of threat agents, their capabilities and knowledge representation according to business assets and the ability to replicate this model in future tests with the same results.

We found that GMA is a SAT that focuses mostly on modeling not quantified complex issues, such as threat modeling. Therefore, we applied GMA in our threat modeling approach, named iModeling Universe attributes, to automatically generate predictive scenarios.

The iModeling Universe of attributes proposal focuses on the clear identification of critical characteristics within cyber security incidents, such as agent profiling, attack profiling and impact profiling. The iModeling Universe of attributes can be applied to a wide range of Internet connected devices and to a wider range of organizations within the modern society. In this research we present three distinct application scenarios of iModeling Universe of attributes proposal: (1) Penetration testing mapping; (2) Cybercriminal investigation; (3) Cyber risk analysis.

- The Penetration testing mapping offers Pentesters the possibility to understand the Pentest from two different perspectives: defensive and offensive. The defensive perspective focuses on the attackers and attempts to understand attacks, identifying vulnerabilities and developing a defensive strategy. The objective is to identify attack approaches and minimize the risk of attack success. The offensive perspective focuses on the defenders and attempts to understand defenses, identifying weaknesses and developing an offensive strategy. The objective is to exploit defenses and minimize the risk of attack failure.

- The Cybercriminal investigation applicability offers the possibility to collect evidences found on the cybercrime scene and input it on iModeling Universe of attributes. It results in the combination of possible strategies of Cybercriminal investigation. Modeling cybercrimes allows to understand how cybercrimes are committed (root causes) and to reflect about adequate approaches to investigate cybercrime scenes.
- The Cyber risk analysis offers a full-scale view of organization's cyber risks over time and may serve as a roadmap for business resilience by improving their cybersecurity measures. With the iModeling Universe of attributes it is possible to identify the risks that a successful cyber-attack have on the organization's critical assets and processes. By understanding their cyber risk exposure, organizations can reduce their financial losses and increase their cybersecurity measures. The use of iModeling Universe of attributes for cyber risk assessment allows organizations to determine security policies, analyze plausible cyber scenarios and evaluate their impact within the organization. With the iModeling Universe of attributes output, organizations can make more informed business decisions such as evaluating security measures cost-benefit, regulatory compliance, managing the cyber risk, among others.

In addition, as proof-of-concept we applied the iModeling Universe of attributes on these three different contexts of application which provided a potential mechanism for its validation.

Importantly, the results of this research also allowed the creation of iPentest methodology, in which it is integrated the iModeling Universe of attributes, which is a potential methodology for improving PTES. The iPentest proposal is a new approach to execute the first phase of Penetration Tests that offers a better understanding of customer's needs and the possibility to direct the Pentest towards specific scenarios. Ideally, these findings should be replicated in further studies for its validation.

Overall, our results demonstrate a broad implication of Intelligence techniques in the Penetration tests.

Before answering the research questions, it is important to highlight the main contributions of this research:

(i). Proposal for Intelligence Collection Source (see *Figure 6 – Intelligence Collection Source*);

(ii). Proposal for iPentest methodology (see *Figure 10 – iPentest Methodology*);

(iii). Proposal for the PTES Pre-engagement Interaction phase (see *Figure 11 – iPentest: Planning & iScenario*);

(iv). Proposal approach for the PTES Threat Modeling Phase (see *Figure 14 – iPentest: iModeling Universe of attributes*).

5.1.Answers to the research questions

The central question from this dissertation focused on the creation of a threat modeling model basing on Intelligence techniques: "**Could the Intelligence process be systematized, identifying methodologies, techniques, and tools to build a model for the PTES recommendation Threat's Modeling phase?**". Our conclusion on this subject is that, indeed, it was possible to create a threat modeling approach for the PTES Threat's Modeling phase based on the integration of Intelligence techniques. To reach this conclusion we began this dissertation with the support of the following three sub questions (SQ), which were transversal to the central question:

Sub Question 1 – "Could it be possible to identify common features of application between Intelligence process and other domains?"

Intelligence is currently related to the process of transforming data into information, and information into knowledge. Intelligence is the key for operational and strategic decision making. Therefore, Intelligence can be applied to any domain that needs data and information analysis, such as Businesses, Medical Diagnosis, Criminal Investigation, Computer Sciences Security, among others. Therefore, it was possible to identify common features of application between Intelligence and Penetration Tests. For instance, it was possible to correlate the Pre-engagement Interactions and Threat Modeling phases of PTES

with the Intelligence cycle, resulting in the iPentest methodology (Figure 10 – iPentest methodology), which is our proposal for PTES improvement.

Sub Question 2 – "Could it be possible to identify methodologies, techniques, and tools that better adapt to specific Intelligence needs?"

Intelligence products are categorized into different categories (see *Figure 3 – Intelligence Products*) and are distinguished by the purpose for which Intelligence was produced. We identified several robust analytic techniques (see *Figure 8 – Structured Analytic Techniques*) used for information and Intelligence analysis. These techniques are directed toward different purposes (see *Figure 9 – Selecting the right technique*). Regarding this finding, we proposed a methodology that offers Pentesters an approach to optimize the first interactions within a customer (see Planning & iScenario from "*Figure 10 – iPentest Methodology").* The iPentest Planning & iScenario phase uses the concepts of the Planning & Directing phase from Intelligence cycle, offering Pentesters an approach for a better understanding of customer's needs. Regarding the existing techniques and their specific application to Intelligence needs, it was also possible to create an approach that offers Pentesting' customers the possibility to select specific scenarios. Those scenarios were constructed based on the techniques that better adapt to specific Intelligence needs (see *Figure 12 – iPentest: Planning & iScenario SAT*).

Sub Question 3 – "Could it be possible to apply Intelligence methodologies and techniques to build a Threat Modeling model?"

It was possible to create a threat modeling approach using the GMA as the engine behind iModeling Universe of attributes (see *Figure 14 – iPentest: iModeling Universe of attributes*). GMA is a dynamic modeling method which can be used to identify and investigate the total set of possible relations contained in a given problem complex. Therefore, GMA can be applied on the creation of threat modeling models. Although, the application of GMA in iModeling Universe of attributes is a proof-of-concept, which permits to automatically profile the attack, allowing to better understand its impact on business assets and processes and to uncover the attack agent characteristics.

5.2.Research Limitations

During this research we had difficulties on finding scientific publications regarding PTES and Intelligence. Most of the bibliographic references about Intelligence are books of ex-officials of the secret services or military documents publicly available. We found just a few scientific articles regarding PTES and much less regarding Intelligence. Consequently, we did not find references merging both fields. This resulted in an increased time spent on searching to obtain reliable sources of information.

Another limitation that stood out during this research was the lack of Portuguese specialists on the Intelligence field. We had some contributions from companies and professors on the Pentesting field but on the Intelligence field we just found experts in OSINT information gathering. However, to minimize the lack of national experts we collected information about Intelligence and threat modeling from several international and reliable sources, such as official secret agencies' online libraries and Intelligence analysts' forums.

We believe that, even with the limitations of information and specialists, it was possible to compile in this dissertation a basis for the correlation between the concepts of Penetration Test and Intelligence, which we hope that will serve as a motivation for future research projects.

5.3.Recommendations and Future Research

Analyzing all the issues addressed in this research, we consider relevant to mention some recommendations and future research:

- The iPentest methodology proposes an improvement of the Pre-engagement Interaction phase and Threat Modeling phase from PTES, which we named in iPentest methodology as Planning and Threat Modeling phase.
- The iPentest Planning phase offers to Pentesters a structured thinking toolkit which increases the Pentesting planning efficiency and the possibility to execute the Pentesting directing it to specific scenarios (iScenario). However, this research needed to be delimitated to certain goals and it was not possible to validate the proposal. Therefore, future researches should be conducted in more realistic settings in order to consider the potential effects of the iPentest Planning & iScenario proposal on Penetration Tests.
- The iPentest Threat Modeling phase offers a threat modeling approach named iModeling Universe attributes. This approach defines a framework that allows to identify

organization's assets; identify which systems comprise those assets and how they may compromise them; identify potential threat agents; and identify the impact if those assets are compromised. However, we believe that future research should look for possible improvements to the attributes that composes iModeling Universe of attributes.

- Additionally, future research should consider the potential effects of using the GMA to make the iModeling Universe of attributes generate threat modeling scenarios automatically. Future studies could fruitfully explore this issue by examining the internal relation between the attributes from iModeling Universe of attributes. This is the key component in future research to overcome the uncertainty of the results.
- Future research should continue to explore iModeling universe of attributes aiming to develop a computer software for predictive threat modeling scenarios with a high degree of accuracy.
- The human interaction with technology is a complex problem and this complexity increases every day. Consequently, we believe the threat modeling will become a foundation for implementing detailed technical, organizational or legal mitigations and for increasing the reliability of our decisions. We believe that cyber threat modeling should be considered in future research to evaluate its potential socioeconomic effects in modern society.
- We conclude that our iPentest methodology proposal fits today's incident security issues. However, with the uncontrollable speed of technology, soon iModeling universe of attributes must be adapted to new types of threats and be prepared to protect different critical assets and operating in socio-technical systems. There are plenty of new vulnerabilities appearing every day, so there will always be question marks and loose ends on the security of Internet-connected devices.
- Additionally, with the extensibility of computers it is possible to program everything around us to become a computer which can do almost everything. However, there are large concerns related to extensible systems: first, those systems are hard to secure because programmers can't anticipate every flaw; second, they depend on the digital world so they can't be externally limited; third, the extensibility means that every system can be upgraded with new features, and those upgrades may contain new vulnerabilities. We are facing a complex problem where it is urgent to be prepared to deal with all kinds of threats, such as the Internet + threats. The impact of these threats can become catastrophic and we must set a strategy to minimize negative consequences (**Schneier, 2018**).

- Founding on iModeling Universe of attributes, future research should be devoted to the development of Internet + threat modeling. This does not mean that our research is incomplete or outdated, rather we prefer to say that it is difficult to create a solution that keeps pace with technological advances. We deeply believe that the information compilated on this research may serve as motivation for further and divergent researches.

6. BIBLIOGRAPHIC REFERENCES

Analyst-IC Associate Teams Program. (2012). **Probing the Implications of Changing the Outputs of Intelligence.** Studies in Intelligence.

AR 380-5. (1988). **Information Security Program.** Headquarters. Available: < *https://fas.org/irp/doddir/army/ar380-5/*>. [Consult. June 2017].

Baybutt, Pl. (2003). **An Asset-based Approach for Industrial Cyber Secuirty Vulnerability Analysis.** Primatech, Inc.

Bergeron, B. (2003). **Essentials of Knowledge Management.** New Jersey: Wiley. Available: <*http://www.cos.ufrj.br/~jano/LinkedDocuments/_papers/aula06/Wiley%20-%20Essentials%20of%20Knowledge%20Management.pdf*>. [Consult. June 2017].

Bimfort, M. T. (1958). **A Definition of Intelligence.** Studies in Intelligence.

Box, G. E. P. and G. C. Tiao (1992). **Bayesian Inference in Statistical Analysis.** Wiley Classics Library ed. Wiley-Interscience.

CJCSI 3370.01. (2016). **Target Development Standards.** Defense Technical Information Center (DTIC). Department of Defense. Available: <*https://fas.org/irp/doddir/dod/cjcsi3370_01.pdf*>. [June 2017].

CJCSM 3314.01A. (2012). **Intelligence Planning.** Joint Intelligence Operations Center (JIOC).

Clark, R. M. (2007). **Intelligence Analysis: A Target-Centric Approach.** CQ Press: Washington, DC.

Cleave, M. K. V. (2015). **What is Counterintelligence? A Guide to Thinking and Teaching about CI**. Guide to the Study of Intelligence. Journal of U.S. Intelligence Studies, Vol 20.

Coyle, R.G.; Y. C. Yong (1996). **A Scenario Projection for the South China Se***a.* Futures 28 (3), 269-283.

Črnčec, D. (2009). **A New Intelligence Paradigm and the European Union**. Journal of Criminal Justice and Security. University of Maribor: Slovenia.

CVE Details (2017). **The Ultimate Security Vulnerability Datasource**. Available online in: <*https://www.cvedetails.com/vulnerabilities-by-types.php*>. [Consult. March 2018].

Day, T., Gibson, H., Ramwell, S. (2016). **Fusion of OSINT and Non-OSINT Data**. In: Akhgar B., Bayerl P., Sampson F. (eds) Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications. Springer, Cham.

Dinis, B. (2013). **Execução de testes de penetração em redes usando a recomendação Penetration Testing Execution Standard.** ISCTE-IUL. Departamento de Ciências e Tecnologias da Informação.

ENISA (2018). **Threat Landscapes Report 2017: 15 Top Cyber-Threats and Trends.** European Union Agency for Network and Information Security. Available: <*https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/.../fullRepo...*>. [Consult. May 2018].

Europol. (2010). **Europol Information Management**. File no: 2510-271. Available: <*http://euro-police.noblogs.org/gallery/3874/Europol%20Products%20and%20Services-Booklet.pdf*>. [June 2017].

FBI (2017). **Public Service Announcement: Consumer Notice: Internet-Conneccted Toys could presente privacy and contact concerns for children**. Available: <*www.ic3.gov/media/2017/170717.aspx*>. [Consult. July 2017].

Fiães, L. (2014). **Intelligence e Segurança Interna.** Instituto Superior de Ciências Policiais e Segurança Interna.

FIRST (2017). **Common Vulnerability Scoring System v3.0: Specification Document.** Available online in: <*https://first.org*> [Consult. March 2018].

FM 2-22.3 (2006). **Human Intelligence Collector Operations.** Headquarters, Department of the Army.

Gandhi, R., Sharma, A., Mahoney, W., Laplante, P. (2011). **Dimension of Cyber-Attacks: Cultural, Social, Economic, and Political**. IEEE Technology and Society Magazine.

Gibson, S. D. (2004). **Open Source Intelligence.** The RUSI Journal.

Goldman, J. (2006). **Words of Intelligence**. A Dictionary. Maryland: The Scarecrow Press.

Grabo, C. M. (2010). **Handbook of Warning Intelligence.** Assessing the Threat to National Security. Plymouth: The Scarecrow Press.

Graça, P.B. (2010). **Mundo Secreto: História do presente e Intelligence nas Relações Internacionais.** Lisboa: Instituto de Informações e Segurança de Angola.

Granger S. (2001). **Social engineering fundamentals, Part I: hacker tactics**. SecurityFocus.

Harrison, K., White, G. (2011). **A Taxonomy of Cyber Events Affecting Communities**. Center Infrastructure Assurance and Security Computer Science. Institute for Cyber Security.

Hedley, J. H. (2007). **The Challenges of Intelligence Analysis.** In L. K. Johnson (Ed.), Strategic Intelligence. Understanding the Hidden Side of Government. Westport, Connecticut: Praeger Security International.

Herzog, P. (2001). **Open Source Security Testing Methodology Manual.** Institute of Security and Open Methodologies.

Heuer, R. J. Jr., Jr., Pherson, R. H. (2011). **Structured Analytic Techniques for Intelligence Analysis**. CQ Press: Washington, DC.

Heuer, R.J., Jr., and R.H. Pherson. (2014). **Structured Analytic Techniques for Intelligence Analysis**. CQ Press: Washington, DC.

Hitz, F. P. (2007). **Human source intelligence**. In L. K., Johnson (Ed), Handbook of Intelligence Studies. London: Routledge.

Howard, J. D., Longstaff, T. A. (1998). **A Common Language for Computer Security Incident**. Sandia National Laboratories;

IEEE. (2000). **The Authoritative Dictionary of IEEE Standards Terms.** Seventh Edition.

International Association of Chiefs of Police. (2002). **Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Federal, State, and Local Levels.** A Summit Report. Alexandria, Virginia: IACP.

ISO/IEC 31000:2018**. Risk Management: Guidelines.**

ISSAF. (2006). **Information Systems Security Assessment Framework**. Open Information Systems Security Group.

ITACG. (2011). **Intelligence Guide for First Responders.** National Counterterrorism Center.

Johnson, L. K. (2007). **Appendix D. Categories of Finished Intelligence and the Major Products.** In Strategic Intelligence. The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government. Westport, Conneticut: Praeger Security International. Available: < *https://fas.org/irp/doddir/dod/jp1_02.pdf*>. [Consult. June 2017].

JP 1-02. (2016). **Department of Defense Dictionary of military and Associated Terms.** Defense Technical Information Center (DTIC). Department of Defense. Available: <*http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf*>. [Consult. June 2017].

JP 2-0. (2013). **Joint Intelligence.** Defense Technical Information Center (DTIC). Department of Defense. Available: <*http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf*>. [Consult. June 2017].

JP 2-01. (2012). **Joint and National Intelligence Support to Military Operations.** Defense Technical Information Center (DTIC). Department of Defense. Available: <*http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf*>. [Consult. June 2017].

JP 3-60. (2013). **Joint Targeting.** Defense Technical Information Center (DTIC). Department of Defense. Available: <*https://www.aclu.org/files/dronefoia/dod/drone_dod_jp3_60.pdf*>. [Consult. June 2017].

Kent, S. (1949). **Strategic Intelligence for American World Policy**. Princeton, New Jersey: Princeton University Press.

Khan, D. (2009). **An Historical Theory of Intelligence.** London: Routledge.

Krizan, L. (1999). **Intelligence Essentials for Everyone**. Washington, D.C.: Joint Military Intelligence College.

Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2015). **Advanced social Engineering attacks.** Journal of Information Security and Applications 22.

Lahneman, W.J. (2010). **The Need for a New Intelligence Paradigm.** International Journal of Intelligence and CounterIntelligence. Vol 23.

Lefebre, M. S. (2004). **A Look at Intelligence Analysis**. International Journal of Intelligence & Counter Intelligence.

Lough, DL. (2001) **A taxonomy of computer attacks with applications to wireless networks**. PhD thesis, Virginia Polytechnic Institute and State University.

Lowenthal, M (2006). **Open-source intelligence: New myths, new realties**. Intelligence and the national security strategist, Rowman and Littlefield Publishers Inc, Oxford.

Lowenthal, M. M. (2008). **Intelligence: From Secrets to Policy.** Washington, DC: CQ Press.

Mangio, C. A., & Wilkinson, B. J. (2008). **Intelligence Analysis: Once Again**. In Aggregating the Intelligence Studies Literature: A Compendium Project Panel Analysis: Themes, Issues and Divergent Views. San Francisco, California.

McDowell, D. (2009). **Strategic Intelligence. A Handbook for Practitioners, Managers, and Users.** Maryland: The Scarecrow Press, Inc. Available: <*http://www.e-reading.club/bookreader.php/135870/McDowell_-_Strategic_Intelligence__A_Handbook_for_Practitioners,_Managers_and_Users.pdf*>. [Consult. June 2017].

Mitnick, K. D.; Simon, W. L. (2003). **The Art of Deception: Controlling the Human Element of Security.** W. Publishing., Ed. Indianapolis: Wiley Publishing.

MITRE (2016). **Common vulnerabilities and exposures**. The MITRE Corporation. Available: <*https://cve.mitre.org*>. [Consult. November, 2017].

National Security Act (1947). Available: <*https://history.state.gov/milestones/1945-1952/national-security-act*>. [Consult. June, 2017].

NATO. (2001). **NATO OSINT Handbook**. Norfolk: SACLANT Intelligence Branch. Available: <*http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf*>. [Consult. June 2017].

Nickerson, C., Kennedy, D., Riley, C., Smith, E., Amit, I., Rabie, A., . . . Strand, J. (n.d). **Penetration Testing Execution Standard**. Available: <*http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines*>. [Consult. June 2018].

NIST SP 800-115. (2008). **SP 800-115: Technical Guide to Information Security Testing and Assessment**. Recommendations of the National Institute of Standards and Technology. US Department of Commerce.

Omand, D. (2014). **The Intelligence Cycle**. In Dover, R., Goodman, M. (Eds.) The Routledge Handbook of Intelligence Studies, London: Routledge.

Omand, D.; Bartlett J.; Miller C. (2012). **Introducing Social Media Intelligence (SOCMINT).** Intelligence and National Security. Available: <*http://dx.doi.org/10.1080/02684527.2012.716965*>. [Consult. June 2017].

OSINT FMI 2-22.9 (2006). **Open Source Intelligence**. Headquarters, Department of the Army. Washington, DC.

OWASP ASVS. (2016). **Open Web Application Security Project**: **Application Security Verification Standard 3.0.1.** Available: <*https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project*>. [Consult. June 2017].

Pherson Associates (2016). **Handbook of Analytic Tools and Techniques.** Pherson Associates, LLC.

Pherson, H. R. (2015). **Strategic Foresight: Nine Techniques for Business and Intelligence Analysis.** Globalytica, LLC.

Platt, W. (1957). **Produção de Inteligência Estratégica.** Nova York: Frederick A. Praeger.

Random, R. A. (1958). **Intelligence as a Science**. Studies in Intelligence.

Rhyne, R. (1981). **Whole-Pattern Futures Projection, Using Field Anomaly Relaxation**. Technological Forecasting and Social Change 19, 331-360.

Richelson, J. T. (2007). **The technical collection of intelligence**. In L. K., Johnson (Ed), Handbook of Intelligence Studies. London: Routledge.

Ritchey, T. (2011). **Modeling Alternative Futures with General Morphological Analysis**. Spring: World Future Review.

Schneier, B. (2018). **Click Here to Kill Everybody: Security and Survival in a Hyper-connected World**. W. W. Norton & Company.

Schulsky, A. N., & Schmitt, G. J. (2002). **Silent Warefar. Understanding the World of Intelligence**. Washinton, D.C.: Brasey's Inc.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wiu, Q. (2009). **AVOIDIT: A Cyber Attack Taxonomy**. Department of Computer Science, University of Memphis.

SIRP. Available: <*https://www.sirp.pt/quem-somos/faqs*>. [Consult. June, 2017].

Stanton, J. M., Stam, K. R., Mastrangelo, P., Jolton, J. (2005). **Analysis of end user security behaviors**. Computers and Security, v24, n2. Available: <*http://dx.doi.org/10.1016/j.cose.2004.07.001*>. [Consult. November, 2017].

UNODC. (2010). **Criminal Intelligence: Manual for Front-line Law Enforcement.** United Nations Office on Drugs and Crime: Vienna. United Nations, New York.

Walters, V. (1978). **Silent Missions.** Garden City, NY: Doubleday.

Warner, M. (2002). **Wanted: A Definition of "Intelligence".** Studies in Intelligence. Available: <*https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html*>. [Consult. June, 2017].

West, N. (2006). **Historical Dictionary of International Intelligence.** Historical Dictionaries of Intelligence and Counterintelligence, No. 4. The Scarecrow Press: Oxford.

Zwicky, F. (1969). **Discovery, Invention, Research Through the Morphological Approach**. Toronto: The Macmillan Company.

7. ANNEXES

Annex I – PTES: Pre-Engagement Interactions

PTES Pre-Engagement Interactions Phase is divided into seven sections: 1) Scoping, 2) Goals, 3) Testing Terms & Definitions, 4) Questionnaires, 5) Establish lines of Communication, 6) Rules of Engagement, and 7) Capabilities and Technology in place, as represented in "*Figure 22 – Pre-Engagement Interactions Phase mind map*".

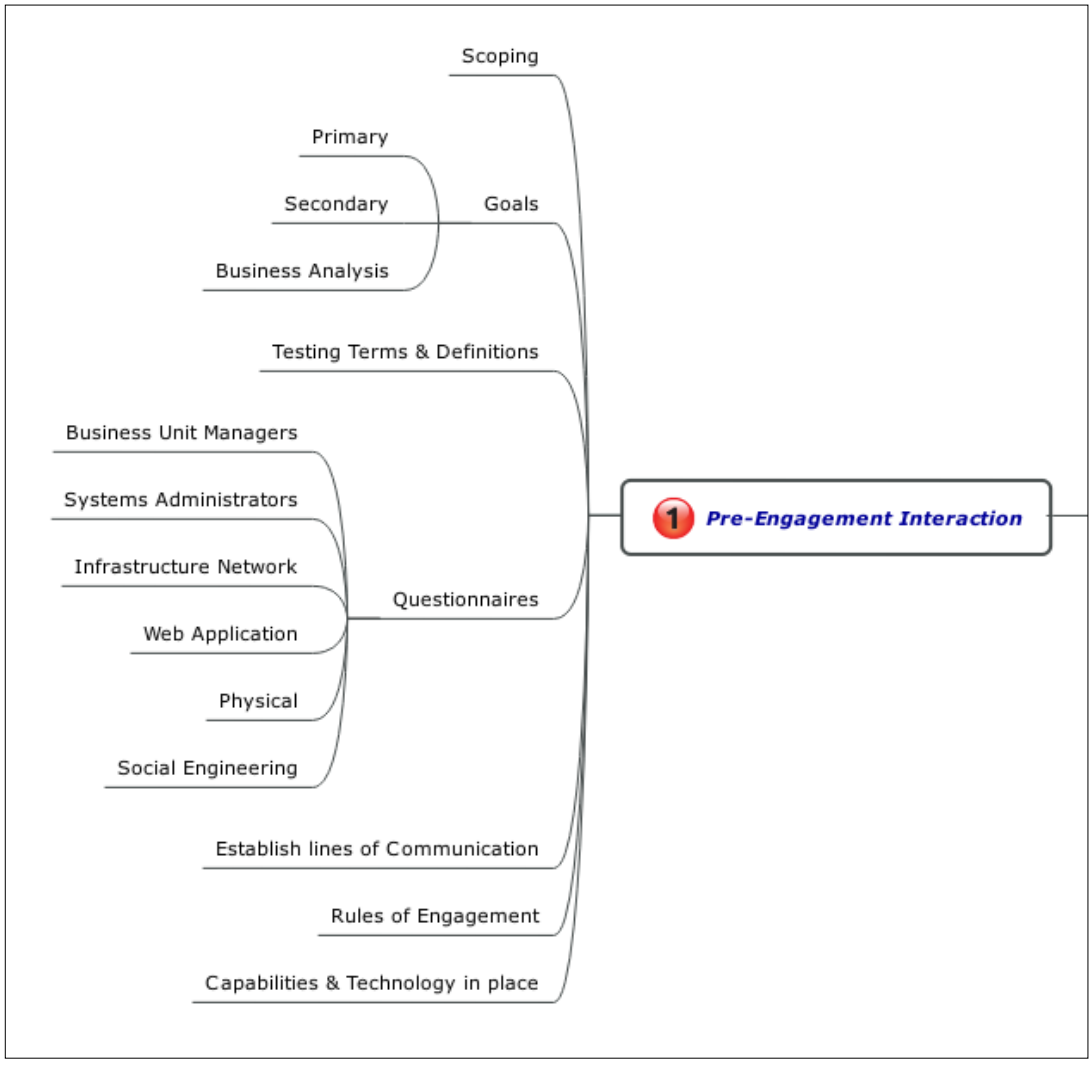

Figure 22 – Pre-Engagement Interactions Phase mind map[16]

[16] Note. **Nickerson et al., n.d.**

Annex Ia – Pre-Engagement Interactions: Questionnaires

A PTES begins with an initial communication with the client through a set of questions that have to be answered in order to accomplish the first phase. These questions are directed for specific targets: Business Unit Managers, System Administrators, and depends on the object under analysis. The following are sample questions which should be asked to extract relevant information. However, it is suggested to complement those sample questions with additional questions (**Nickerson et al., n.d.**):

1. QUESTIONS FOR BUSINESS UNIT MANAGERS

1.1. Is the manager aware that a test is about to be performed?
1.2. What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?
1.3. Are testing and validation procedures to verify that business applications are functioning properly in place?
1.4. Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?
1.5. Are Disaster Recovery Procedures in place for the application data?

2. QUESTIONS FOR SYSTEMS ADMINISTRATORS

2.1. Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
2.2. Are there systems on the network which the client does not own, that may require additional approval to test?
2.3. Are Change Management procedures in place?
2.4. What is the mean time to repair systems outages?
2.5. Is any system monitoring software in place?
2.6. What are the most critical servers and applications?
2.7. Are backups tested on a regular basis?
2.8. When was the last time the backups were restored?

3. NETWORK PENETRATION TEST

3.1. Why is the customer having the penetration test performed against their environment?
3.2. Is the penetration test required for a specific compliance requirement?

3.3. When does the customer want the active portions (scanning, enumeration, exploitation, etc...) of the penetration test conducted?
  3.3.1. During business hours?
  3.3.2. After business hours?
  3.3.3. On the weekends?
3.4. How many total IP addresses are being tested?
  3.4.1. How many internal IP addresses, if applicable?
  3.4.2. How many external IP addresses, if applicable?
3.5. Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?
3.6. In the case that a system is penetrated, how should the testing team proceed?
3.7. Perform a local vulnerability assessment on the compromised machine?
  3.7.1. Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?
  3.7.2. Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc/shadow on Unix machines)?

4. WEB APPLICATION PENETRATION TEST

4.1. How many web applications are being assessed?
4.2. How many login systems are being assessed?
4.3. How many static pages are being assessed? (approximate)
4.4. How many dynamic pages are being assessed? (approximate)
4.5. Will the source code be made readily available?
4.6. Will there be any kind of documentation?
  4.6.1. If yes, what kind of documentation?
4.7. Will static analysis be performed on this application?
4.8. Does the client want fuzzing performed against this application?
4.9. Does the client want role-based testing performed against this application?
4.10. Does the client want credentialed scans of web applications performed?

5. WIRELESS NETWORK PENETRATION TEST

5.1. How many wireless networks are in place?
5.2. Is a guest wireless network used? If so:
  5.2.1. Does the guest network require authentication?
  5.2.2. What type of encryption is used on the wireless networks?
  5.2.3. What is the square footage of coverage?
  5.2.4. Will enumeration of rogue devices be necessary?

5.2.5. Will the team be assessing wireless attacks against clients?

5.2.6. Approximately how many clients will be using the wireless network

6. PHYSICAL PENETRATION TEST

6.1. How many locations are being assessed?

6.2. Is this physical location a shared facility? If so:

6.2.1. How many floors are in scope?

6.2.2. Which floors are in scope?

6.3. Are there any security guards that will need to be bypassed? If so:

6.3.1. Are the security guards employed through a 3rd party?

6.3.2. Are they armed?

6.3.3. Are they allowed to use force?

6.4. How many entrances are there into the building?

6.5. Is the use of lock picks or bump keys allowed? (also consider local laws)

6.6. Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?

6.7. What is the square footage of the area in scope?

6.8. Are all physical security measures documented?

6.9. Are video cameras being used?

6.9.1. Are the cameras client-owned? If so:

6.9.1.1. Should the team attempt to gain access to where the video camera data is stored?

6.10. Is there an armed alarm system being used? If so:

6.10.1. Is the alarm a silent alarm?

6.10.2. Is the alarm triggered by motion?

6.10.3. Is the alarm triggered by opening of doors and windows?

7. SOCIAL ENGINEERING

7.1. Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?

7.2. Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?

7.3. Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so:

7.3.1. How many people will be targeted?

Annex II – PTES: Intelligence Gathering

PTES Intelligence Gathering phase is divided into five sections: 1) Target selection, 2) OSINT, 3) Covert Gathering, 4) Foot printing, and 5) Identify Protection Mechanism, as represented in "*Figure 23 – Intelligence Gathering Phase mind map*".

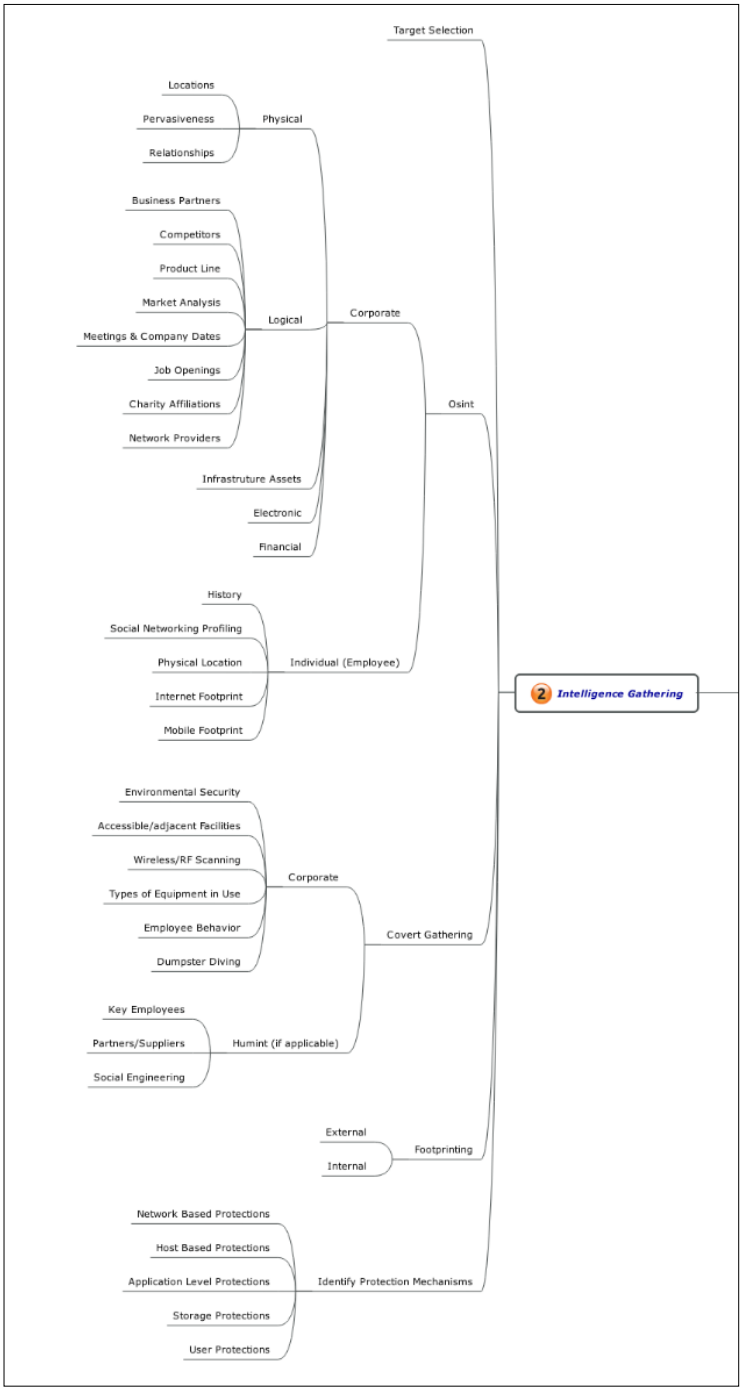

Figure 23 – Intelligence Gathering Phase mind map[17]

[17] Note. **Nickerson et al., n.d.**

Annex III – PTES: Threat Modeling

PTES Threat Modeling phase is divided into six sections: 1) Business Assets Analysis, 2) Business Processes Analysis, 3) Threat Agent/Community Analysis, 4) Threat Capability Analysis, 5) Motivation Modeling, and 6) Finding relevant news of comparable organizations, as represented in "*Figure 24 – Threat Modeling Phase mind map*".

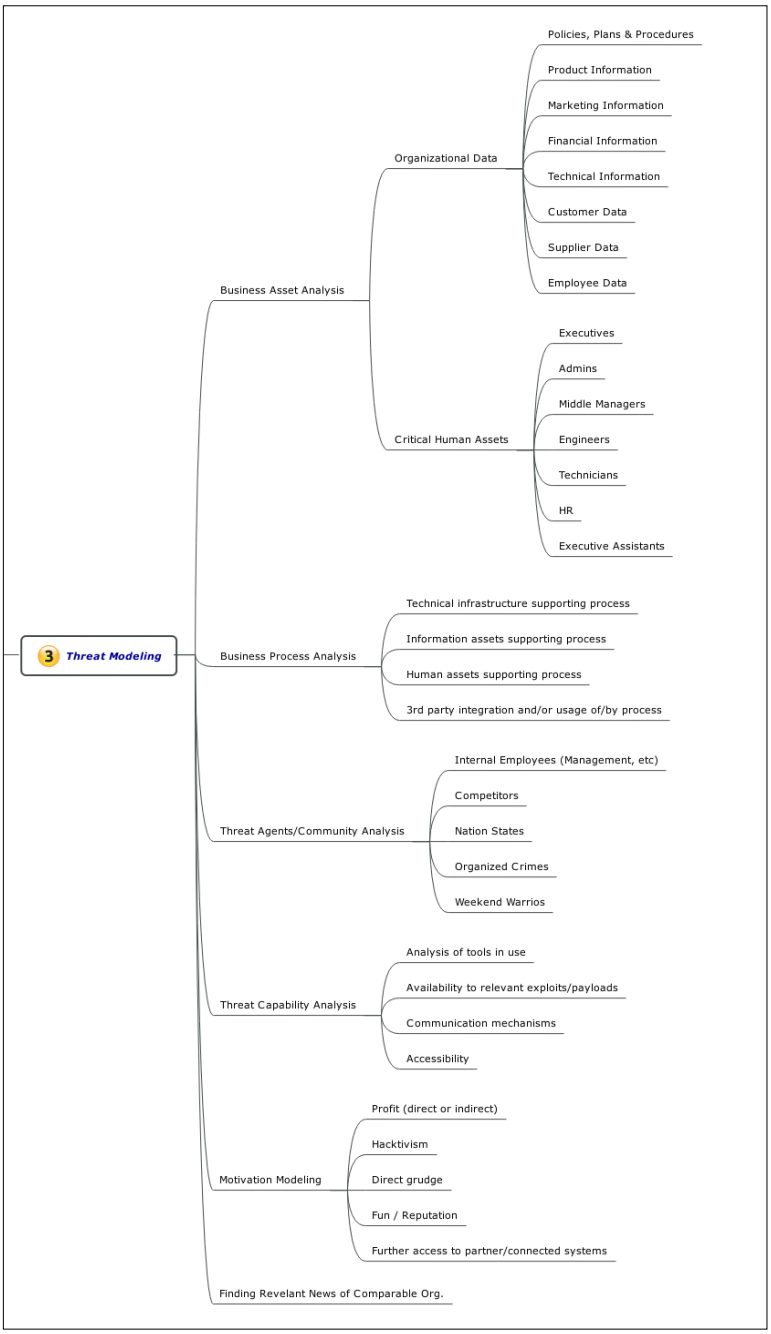

Figure 24 – Threat Modeling Phase mind map[18]

[18] Note. **Nickerson et al., n.d.**

Annex IV - Threat Modeling: Threat Agents/Community Analysis

A clear profiling of the threat agent should be classified in terms of Internal or External threat to the organization. It is also important to understand capabilities and motivations of each agent or community. Some examples of threat agents can be classified as represented in "*Table 9 – Threat Agents/Community*".

INTERNAL	EXTERNAL
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

Table 9 – Threat Agents/Community [19]

The employees can be understood as internal threats. These are the persons who work directly with the targeted company, including those working full-time and/or part-time. In addition to employees, also the cleaning staff and security staff of the physical infrastructure work directly with technological infrastructure devices. Information can be collected from different sources using labored techniques, provided that imagination and creativity allow it. Depending on the position and roles, employees (e.g., chief department, executive) can have more or less access to privileged information. These persons can be influenced by attackers to participate or provide information that facilitates computer systems intrusions or even to act on their own, leading to illegal acts. At last, technological infrastructure information can be compromised due to the employees' negligence or as a result of misinformation.

[19] Note. Adapted from **Nickerson et al., n.d.**

Annex V – Counter-Terrorism Analytical Framework

The CTAF represents an example of structuring key topics for the subsequent collection and analysis of information regarding Terrorism contexts (**CJCSI 3370.01, 2016**).

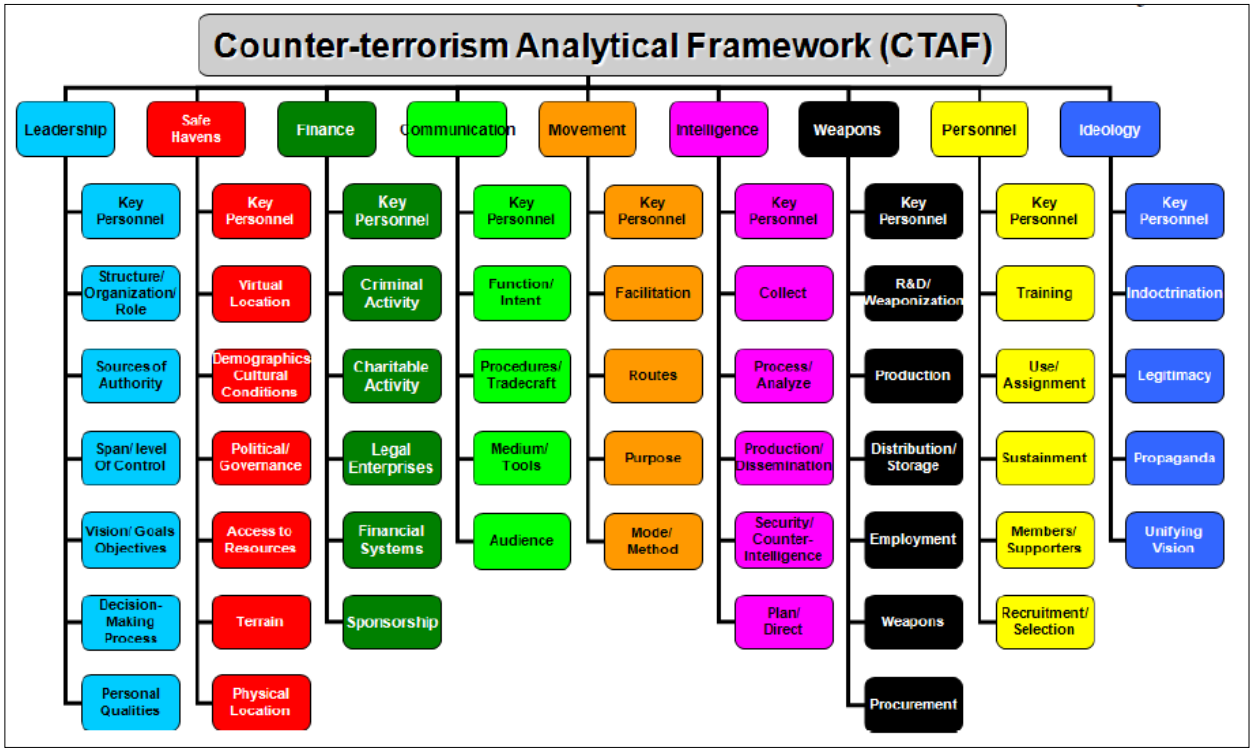

Figure 25 – CTAF[20]

[20] Note. **CJCSI 3370.01, 2016**

Annex VI - Information Classification

Different types of information are distinguished in private information and publicly available information (*Figure 26 – Information Classification*). Private information refers to data and information of a particular individual, group or organization, that is protected from public disclosure, usually classified as Confidential Source. Public information refers to data and information published for public knowledge, which can be legally seen or heard by any casual observer. Sources of information that are not protected from public disclosure are generally classified as Open Source (**OSINT IMF 2-22.9, 2006)**. Data and information resulting from sensitive sources or classified methods, are also classified as shown in *Figure 26 – Information Classification*. except if Intelligence reveals the identity of the source or method **(AR 380-5, 1988**).

TYPE OF INFORMATION	INFORMATION SOURCE	IF COLLECTION MEANS	THEN SOURCE METADATA	THEN INTELLIGENCE REPORT
Private Information	Confidential Source	Overt	Classified or Controlled Unclassified	Classified or Controlled Unclassified
		Clandestine	Classified	
Publicly Available Information	Open Source	Overt	Unclassified	Classified, Controlled Unclassified or Unclassified
		Nonattributable		

Figure 26 – Information Classification[21]

[21] Note. Adapted from **OSINT FMI 2-22.9, 2006**

Annex VII – Evaluation Matrix

Data and information must be subject to an evaluation, ensuring its consistency, usefulness and interpretation through the reliability of sources and credibility of the information through evaluations matrices. The "*Figure 27 – Information Metric*" is seen as a qualitative metric to evaluate the confidence level of sources and likelihood of information.

INFORMATION CREDIBILITY			SOURCE RELIABILITY		
1	**Confirmed**	Confirmed by other independent sources; logical; consistent with other information on the subject; accuracy is not in doubt.	A	**Reliable**	No doubt of authenticity, trustworthiness; has a history of complete reliability; demonstrates adherence to known professional standards and verification processes.
2	**Probably True**	Not Confirmed; logical; consistent with other information on the subject; known personally but not known personally to the official passing it on.	B	**Usually Reliable**	Minor doubt about authenticity; trustworthiness; has a history of valid information most of the time; may not have history of adherences to professionally accepted standards but generally identifies what's is know about sources feeding any broadcast.
3	**Possibly True**	Not confirmed; possible but not logical; no other information on the subject.	C	**Fairly Reliable**	Doubt of authenticity and trustworthiness but has provided valid information in the past.
4	**Improbable**	Not confirmed; not logical; not known personally but corroborated by other information recorded.	D	**Not Usually Reliable**	Significant doubt about authenticity and trustworthiness but has provided valid information in the past.
5	**Misinformation**	False; not logical; contradicted by other information on the subject; confirmed by other independent sources.	E	**Unreliable**	Lacking in authenticity and trustworthiness; history of invalid information.
6	**Cannot be Judged**	No basis exists for evaluating the validity of the information.	F	**Cannot be Judged**	No basis exists for evaluating the reliability of the source; new information source.

Figure 27 – Information Metric[22]

Further, the information is classified through evaluation matrices, which can be 4x4, 5x5, 6x6, depending on the context in which they are inserted. The "*Figure 28 – Evaluation Matrix*" shows an example of a 4x4 matrix:

			SOURCE EVALUATION			
			A	**B**	**C**	**D**
		RATING	Reliable	Usually Reliable	Fairly Reliable	Cannot be assessed
INFORMATION EVALUATION	**1**	Confirmed	**A1**	**B1**	C1	D1
	2	Probably True	**A2**	**B2**	C2	D2
	3	Improbable	A3	B3	C3	D3
	4	Cannot be assessed	A4	B4	C4	D4

Figure 28 – Evaluation Matrix[23]

According to this matrix, we find that A1 information is consistent, because it is confirmed by other sources and its source of information is reliable. Therefore, A1 information is more credible than the others. As we go through the remaining columns and rows, the information has less consistency and confidence, not being so reliable. This assessment should be dynamic, since changes in the context or in searching for new information may alter previous evaluations (**Fiães, 2014**).

[22] Note. Adapted from **Europol, 2010; JP 2.0, 2013.**
[23] Note. Adapted from **Europol, 2010; JP 2.0, 2013.**

Annex VIII– Qualitative Language

Typically, hypotheses result from incomplete data or information. It is not possible to confirm the possibility of occurrence of a certain event, which is equal to 1 or 0. But it is possible to determine if an event occurs or if an event does not occur. So, two events are mutually exclusive, that is, the occurrence of one of them excludes the occurrence of the other. Consequently, the probability of one event to occur is equal to the sum of the two probabilities (**Box & Tiao, 1992**)[24]. Therefore, in this context the probability of occurrence of a certain event, the links between events, or the degree of confidence of hypotheses, is measured through a qualitative language, as represented in "*Figure 29 – Estimative Language*" (**CIA, 2008**).

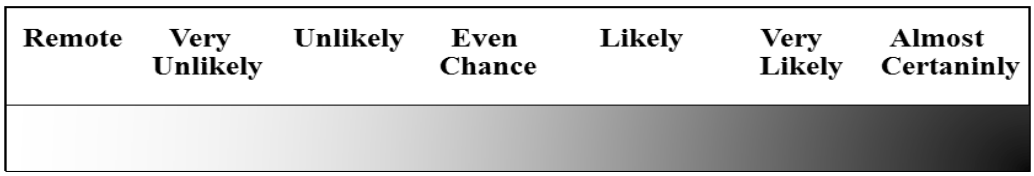

Figure 29 – Estimative Language[25]

While the labels Almost Certainly, Very Likely, and Likely are used as indicators of great probability of occurrence, the labels Unlikely, Very Unlikely, and Remote are used for less probable occurrences. We can also attribute to these terms the mathematical estimate of probabilities, as represented in "*Figure 30 – Estimative Probability*" (**Platt, 1957; CIA, 2008**).

ESTIMATIVE PROBABILITY			
	100% Certaninly		
	The General Area of Possibility		
	93%	give or take about 6%	Almost Certaninly
	75%	give or take about 12%	Very Likely
	50%	give or take about 10%	Even Chance
	30%	give or take about 10%	Unlikely
	7%	give or take about 5%	Very Unlikely
	0% Impossible		

Figure 30 – Estimative Probability[26]

[24] These rules are based on the principles of Bayesian Inferences applied to statistical analysis, which allows the deduction of uncertain events (**Box & Tiao, 1992**).
[25] Note. Adapted from **National Intelligence Estimative (2007).**
[26] Note. Adapted **from Platt, 1957; CIA 2008.**

Regarding the degree of confidence of formulated hypothesis, evaluations and estimates are supported by information which quality of information and sources varies according to their scope. The degree of confidence can be characterized in three distinct levels of confidence: High, Moderate, and Low (*Figure 31 – Hypotheses Credibility*).

HYPOTHESES CREDIBILITY		
1	**High Confidence**	Generally indicates that the assumptions are derived from high-quality information and / or the nature of the issue has a solid judgment. Still, a hypothesis with a "high" level of confidence is not a fact or a certainty, yet it is intrinsic to the risk of being wrong.
2	**Moderate Confidence**	Indicates that the information is credible and plausible, but is not of sufficient quality to guarantee a higher level of confidence.
3	**Low Confidence**	Indicates that the credibility or plausibility of the information is questionable. When there is very fragmented and poorly proven information to formulate analytical inferences or when there are significant doubts about the sources of information.

Figure 31 – Hyphoteses Credibility[27]

[27] Note. Adapted **Europol, 2010; JP 2.0, 2013.**

Annex IX– Social Engineering Attacks

SE is the ability of leading human targets to compromise corporate information systems. It assumes two perspectives: directed to Humans or Software. SE attacks include physical, social and technical approaches used in different phases of the attack, as represented in "*Figure 32 – SE Attacks*" **(Granger 2001; Mitnick & Simon, 2002; Mitnick & Simon, 2003; Mouton, et al, 2014; Krombholz, et al, 2015).**

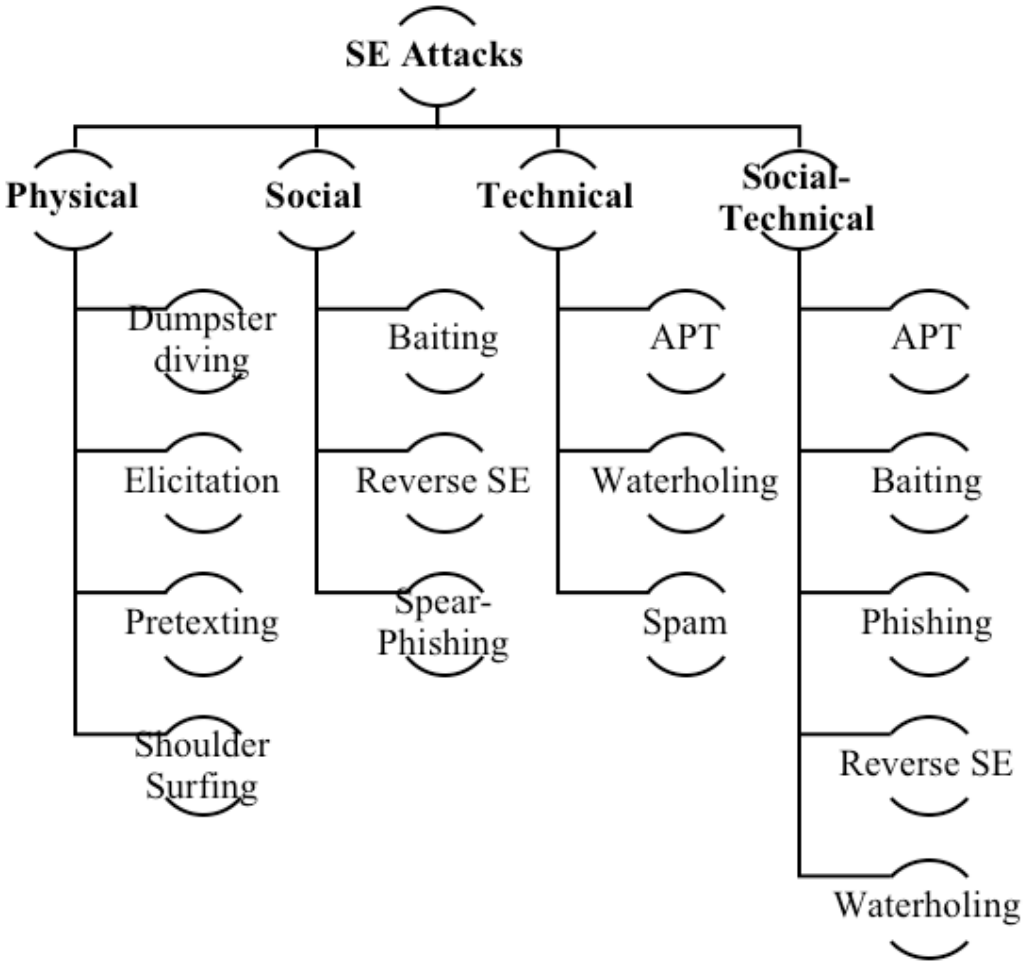

Figure 32 – SE Attacks